Private-Public Partnerships: Legal and Policy Issues

Risk—Cyber Security—Electricity Sector—Supply Chain

Homeland Security Law Institute, 2015

1) Global and U.S. Risks

2) Cyber Security
   c. Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, 2014
   e. Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing, White House, 2015

3) Critical Infrastructure Security: Electricity Sector

4) Critical Infrastructure Security: Supply Chain
      i. Implementation Update, White House, 2013
LETTER FROM THE SECRETARY

June 18, 2014

Pursuant to Section 707 of the Homeland Security Act of 2002 (P.L. 107-296), as amended by the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53), I am pleased to present the following report, The 2014 Quadrennial Homeland Security Review. This report provides a strong analytic and strategic foundation for one of my highest priorities, which is ensuring that the Department invests and operates in a cohesive, unified fashion and makes decisions that strengthen Departmental unity of effort.

Pursuant to congressional requirements, this report is being provided to the following Member of Congress:

The Honorable Michael McCaul
Chairman, House Committee on Homeland Security

The Honorable Bennie G. Thompson
Ranking Member, House Committee on Homeland Security

The Honorable Thomas R. Carper
Chairman, Senate Homeland Security and Governmental Affairs Committee

The Honorable Tom Coburn
Ranking Member, Senate Homeland Security and Governmental Affairs Committee

The first Quadrennial Homeland Security Review report was issued by DHS on February 1, 2010. DHS began work on this second review two years ago and included consultations with subject matter experts across the Federal Government, as well as state, local, tribal, and territorial governments, the private sector, and academic and other institutions.

Since taking office as Secretary of DHS on December 23, 2013, I have reviewed this report, and I concur with its recommendations. Reflecting deep analysis of the evolving strategic environment and outlining the specific strategic shifts necessary to keep our Nation secure, this report reflects the more focused, collaborative Departmental strategy, planning, and analytic capability that is necessary for achieving Departmental unity.

Sincerely,

Jeh Charles Johnson
This page intentionally left blank
EXECUTIVE SUMMARY

In this report, we conclude that we will continue to adhere to the five basic homeland security missions set forth in the first Quadrennial Homeland Security Review report in 2010, but that these missions must be refined to reflect the evolving landscape of homeland security threats and hazards. The Deepwater Horizon oil spill in 2010, Hurricane Sandy in 2012, and the Boston Marathon bombing in 2013 illustrate these evolving threats and hazards. We must constantly learn from them and adapt. The terrorist threat is increasingly decentralized and may be harder to detect. Cyber threats are growing and pose ever-greater concern to our critical infrastructure systems as they become increasingly interdependent. Natural hazards are becoming more costly to address, with increasingly variable consequences due in part to drivers such as climate change and interdependent and aging infrastructure.

Meanwhile, this Nation’s homeland security architecture has matured over the past four years, and we are determined that this progress continue. For example, our law enforcement and intelligence communities are becoming increasingly adept at identifying
and disrupting terrorist plotting in this country. Programs such as TSA Pre✓™ and Global Entry demonstrate the effectiveness and efficiency of risk-based security that can be achieved within budget constraints. It is also worth noting that, in late 2013, DHS received its first unqualified or “clean” audit opinion; this occurred just 10 years after the Department’s formation, which was the largest realignment and consolidation of Federal Government agencies and functions since the creation of the Department of Defense in 1947.

Here are our five basic homeland security missions, revised to address threats and hazards over the next four years:

**Prevent Terrorism and Enhance Security.** Preventing terrorist attacks on the Nation is and should remain the cornerstone of homeland security. Since the last quadrennial review in 2010, the terrorist threat to the Nation has evolved, but it remains real and may even be harder to detect. The Boston Marathon bombing illustrates the evolution of the threat. Through the U.S. Government’s counterterrorism efforts, we have degraded the ability of al-Qa’ida’s senior leadership in Afghanistan and Pakistan to centrally plan and execute sophisticated external attacks. But since 2009, we have seen the rise of al-Qa’ida affiliates, such as al-Qa’ida in the Arabian Peninsula, which has made repeated attempts to export terrorism to our Nation. Additionally, we face the threat of domestic-based “lone offenders” and those who are inspired by extremist ideologies to radicalize to violence and commit acts of terrorism against Americans and the Nation. These threats come in multiple forms and, because of the nature of independent actors, may be hardest to detect. We must remain vigilant in detecting and countering these threats. Given the nature of this threat, engaging the public and private sectors through campaigns, such as “If You See Something, Say Something™” and the Nationwide Suspicious Activity Reporting Initiative, and through partnering across federal, state, local, tribal, and territorial law enforcement will, over the next four years, become even more important.

**Secure and Manage Our Borders.** We must continue to improve upon border security, to exclude terrorist threats, drug traffickers, and other threats to national security, economic security, and public safety. We will rely on enhanced technology to screen incoming cargo at ports of entry and will work with foreign partners to monitor the international travel of individuals of suspicion who seek to enter this country. We will continue to emphasize risk-based strategies that are smart, cost-effective, and conducted in a manner that is acceptable to the American people. We must remain agile in responding to new trends in illegal migration, from Central America or elsewhere. Meanwhile, we recognize the importance of continuing efforts to promote and expedite lawful travel and trade that will
continue to strengthen our economy.

**Enforce and Administer Our Immigration Laws.** We will continually work to better enforce our immigration laws and administer our immigration system. We support common-sense immigration reform legislation that enhances border security, prevents and discourages employers from hiring undocumented workers, streamlines our immigration processing system, and provides an earned pathway to citizenship for the estimated 11.5 million undocumented immigrants in this country. It is indeed a matter of homeland security and common sense that we encourage those physically present in this country to come out of the shadows and to be held accountable. Offering the opportunity to these 11.5 million people—most of whom have been here 10 years or more and, in many cases, came here as children—is also consistent with American values and our Nation’s heritage. We will take a smart, effective, and efficient risk-based approach to border security and interior enforcement and continually evaluate the best use of resources to prioritize the removal of those who represent threats to public safety and national security.

**Safeguard and Secure Cyberspace.** We must, over the next four years, continue efforts to address the growing cyber threat, illustrated by the real, pervasive, and ongoing series of attacks on our public and private infrastructure. This infrastructure provides essential services such as energy, telecommunications, water, transportation, and financial services and is increasingly subject to sophisticated cyber intrusions which pose new risks. As the Federal Government’s coordinator of efforts to counter cyber threats and other hazards to critical infrastructure, DHS must work with both public and private sector partners to share information, help make sure new infrastructure is designed and built to be more secure and resilient, and continue advocating internationally for openness and security of the Internet and harmony across international laws to combat cybercrime. Further, DHS must secure the Federal Government’s information technology systems by approaching federal systems and networks as an integrated whole and by researching, developing, and rapidly deploying cybersecurity solutions and services at the pace that cyber threats evolve. And finally, we must continue to develop cyber law enforcement,
incident response, and reporting capabilities by increasing the number and impact of cybercrime investigations, sharing information about tactics and methods of cyber criminals gleaned through investigations, and ensuring that incidents reported to any federal department or agency are shared across the U.S. Government. In addition, the Federal Government must continue to develop good working relationships with the private sector, lower barriers to partnership, develop cybersecurity best practices, promote advanced technology that can exchange information at machine speed, and build the cyber workforce of tomorrow for DHS and the Nation.

**Strengthen National Preparedness and Resilience.** Acting on the lessons of Hurricane Katrina, we have improved disaster planning with federal, state, local, tribal, and territorial governments, as well as nongovernmental organizations and the private sector; pre-positioned a greater number of resources; and strengthened the Nation’s ability to respond to disasters in a quick and robust fashion. Seven years after Katrina, the return on these investments showed in the strong, coordinated response to Hurricane Sandy. We must continue this progress.

This review recognizes the environment in which we must pursue the homeland security missions over the next four years. To support priority security requirements in a sustainable way, a corollary responsibility for DHS is to become more efficient and effective across a large and decentralized structure. As a Department, we must eliminate duplicative processes, develop common platforms, and purchase single solutions, while pursuing important commitments, such as the recapitalization of the aging Coast Guard fleet. DHS must and will also address the low morale that exists within many of its Components.

Finally, we recognize that we operate at a time when the public’s confidence in the government’s ability to function and work for them is low. DHS is unique among federal agencies for the large, daily engagement it has with the public at airports, seaports, and land ports of entry. Thus, the public’s attitude toward the entire Federal Government can be shaped by interactions with DHS. Over the next four years, DHS will find opportunities to promote confidence in its ability to fulfill its mission.

There is no more important function that a government can provide for its people than safety and security. Through the leadership of our President, and in full partnership with other federal departments and agencies; state, local, tribal, and territorial governments; nongovernmental and private sector organizations; our foreign allies; and the American public, we will continue to work hard in pursuit of the homeland security missions; nothing less than the safety and security of the American people depend on this.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Letter from the Secretary</td>
<td>3</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>5</td>
</tr>
<tr>
<td>1. Legal Requirement for the Review and Report</td>
<td>11</td>
</tr>
<tr>
<td>2. The Purpose of the Second Quadrennial Homeland Security Review</td>
<td>13</td>
</tr>
<tr>
<td>3. The Strategic Environment</td>
<td>17</td>
</tr>
<tr>
<td>4. Guiding Principles</td>
<td>30</td>
</tr>
<tr>
<td>5. Strategic Priorities</td>
<td>33</td>
</tr>
<tr>
<td>• Securing Against the Evolving Terrorism Threat</td>
<td>33</td>
</tr>
<tr>
<td>• Safeguard and Secure Cyberspace</td>
<td>39</td>
</tr>
<tr>
<td>• A Homeland Security Strategy for Countering Biological Threats and Hazards</td>
<td>46</td>
</tr>
<tr>
<td>• A Risk Segmentation Approach to Securing and Managing Flows of People and Goods</td>
<td>53</td>
</tr>
<tr>
<td>• Strengthening the Execution of Our Missions Through Public-Private Partnerships</td>
<td>58</td>
</tr>
<tr>
<td>6. Areas of Ongoing Priority and Emphasis</td>
<td>62</td>
</tr>
<tr>
<td>• Nuclear Terrorism Using an Improvised Nuclear Device</td>
<td>62</td>
</tr>
<tr>
<td>• Immigration</td>
<td>65</td>
</tr>
<tr>
<td>• National Preparedness and the Whole Community Approach</td>
<td>71</td>
</tr>
<tr>
<td>7. Mission Framework In Depth</td>
<td>75</td>
</tr>
<tr>
<td>8. Conclusion</td>
<td>81</td>
</tr>
<tr>
<td>Appendix A: HOMELAND SECURITY ROLES AND RESPONSIBILITIES</td>
<td>83</td>
</tr>
<tr>
<td>Appendix B: PROCESS AND STAKEHOLDER ENGAGEMENT ACTIVITIES</td>
<td>94</td>
</tr>
</tbody>
</table>
This page intentionally left blank
1. LEGAL REQUIREMENT FOR THE REVIEW AND REPORT

Section 707 of the *Homeland Security Act of 2002* (P.L. 107-296), as amended by the *Implementing Recommendations of the 9/11 Commission Act of 2007* (P.L. 110-53), includes the following requirement:

6 U.S.C. 347. QUADRENNIAL HOMELAND SECURITY REVIEW

(a) Requirement

(1) Quadrennial reviews required
In fiscal year 2009, and every 4 years thereafter, the Secretary shall conduct a review of the homeland security of the Nation (in this section referred to as a “quadrennial homeland security review”).

(2) Scope of reviews
Each quadrennial homeland security review shall be a comprehensive examination of the homeland security strategy of the Nation, including recommendations regarding the long-term strategy and priorities of the Nation for homeland security and guidance on the programs, assets, capabilities, budget, policies, and authorities of the Department.

(3) Consultation
The Secretary shall conduct each quadrennial homeland security review under this subsection in consultation with--

(A) the heads of other Federal agencies, including the Attorney General, the Secretary of State, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of the Treasury, the Secretary of Agriculture, and the Director of National Intelligence;

(B) key officials of the Department; and

(C) other relevant governmental and nongovernmental entities, including state, local, and tribal government officials, members of Congress, private sector representatives, academics, and other policy experts.

(4) Relationship with future years homeland security program
The Secretary shall ensure that each review conducted under this section is coordinated with the Future Years Homeland Security Program required under section 454 of this title.

(b) Contents of review
In each quadrennial homeland security review, the Secretary shall--

(1) delineate and update, as appropriate, the national homeland security strategy, consistent with appropriate national and Department strategies, strategic plans, and Homeland Security Presidential Directives, including the National Strategy for Homeland Security, the National Response Plan, and the Department Security Strategic Plan;

(2) outline and prioritize the full range of the critical homeland security mission areas of the Nation;

(3) describe the interagency cooperation, preparedness of Federal response assets, infrastructure, budget plan, and other elements of the homeland security program and policies of the Nation associated with the national homeland security strategy, required to execute successfully the full range of missions called for in the national homeland security strategy described in paragraph (1) and the homeland security mission areas outlined under paragraph (2);

(4) identify the budget plan required to provide sufficient resources to successfully execute the full range of missions called for in the national homeland security strategy described in
(c) Reporting

(1) In general

Not later than December 31 of the year in which a quadrennial homeland security review is conducted, the Secretary shall submit to Congress a report regarding that quadrennial homeland security review.

(2) Contents of report

Each report submitted under paragraph (1) shall include—

(A) the results of the quadrennial homeland security review;

(B) a description of the threats to the assumed or defined national homeland security interests of the Nation that were examined for the purposes of that review;

(C) the national homeland security strategy, including a prioritized list of the critical homeland security missions of the Nation;

(D) a description of the interagency cooperation, preparedness of Federal response assets, infrastructure, budget plan, and other elements of the homeland security program and policies of the Nation associated with the national homeland security strategy, required to execute successfully the full range of missions called for in the applicable national homeland security strategy referred to in subsection (b)(1) of this section and the homeland security mission areas outlined under subsection (b)(2) of this section;

(E) an assessment of the organizational alignment of the Department with the applicable national homeland security strategy referred to in subsection (b)(1) of this section and the homeland security mission areas outlined under subsection (b)(2) of this section, including the Department's organizational structure, management systems, budget and accounting systems, human resources systems, procurement systems, and physical and technical infrastructure;

(F) a discussion of the status of cooperation among Federal agencies in the effort to promote national homeland security;

(G) a discussion of the status of cooperation between the Federal Government and state, local, and tribal governments in preventing terrorist attacks and preparing for emergency response to threats to national homeland security;

(H) an explanation of any underlying assumptions used in conducting the review; and

(I) any other matter the Secretary considers appropriate.

(3) Public availability

The Secretary shall, consistent with the protection of national security and other sensitive matters, make each report submitted under paragraph (1) publicly available on the Internet website of the Department.

(d) Authorization of appropriations

There are authorized to be appropriated such sums as may be necessary to carry out this section.
2. THE PURPOSE OF THE SECOND QUADRENNIAL HOMELAND SECURITY REVIEW

More than 12 years after the attacks of September 11, 2001, the United States is poised to begin a new era in homeland security. Long-term changes in the security environment and critical advances in homeland security capabilities require us to rethink the work DHS does with our partners—the work of building a safe, secure, and resilient Nation.

This new era is defined by both positive and negative factors: the termination of offensive military operations in Iraq and Afghanistan, two of the longest conflicts in U.S. history; the rise of fiscal challenges at home and in partner states; global economic growth, tempered by increased volatility; growth in domestic energy supplies, contrasted with instability in major energy-producing regions; resource constraints in a more densely populated, urbanized world; and rapid technological change that impacts how we live, work, communicate, travel, and access knowledge.
THE PURPOSE OF THE SECOND QHSR

This Quadrennial Homeland Security Review is consistent with, and supports the enduring national interests of the United States, as articulated in our national security strategy:

- The security of the United States, its citizens, and U.S. allies and partners;
- A strong, innovative, and growing U.S. economy in an open international economic system that promotes opportunity and prosperity;
- Respect for universal values at home and around the world; and
- An international order advanced by U.S. leadership that promotes peace, security, and opportunity through stronger cooperation to meet global challenges.

These national interests are inextricably linked and cannot be pursued in isolation.

THE FIVE HOMELAND SECURITY MISSIONS

The first quadrennial review established the five enduring missions of homeland security. This review reaffirms the five-mission structure and updates the missions (detailed in the Mission Framework In Depth section). The updated missions are:

- Prevent Terrorism and Enhance Security;
- Secure and Manage Our Borders;
- Enforce and Administer Our Immigration Laws;
- Safeguard and Secure Cyberspace; and
- Strengthen National Preparedness and Resilience.

Accomplishing these missions requires unity of effort—both across every area of DHS activity and among the numerous homeland security partners and stakeholders. The five missions advance each of the four enduring national interests articulated in the National Security Strategy. Successful accomplishment of

HOMELAND SECURITY VISION

A homeland that is safe, secure, and resilient against terrorism and other hazards, where American interests, aspirations, and way of life can thrive.
these missions results in a secure homeland, fosters a thriving economy, and protects privacy, civil rights, and civil liberties. We pursue enduring national interests and conduct our missions in service to a single homeland security vision: a homeland that is safe, secure, and resilient against terrorism and other hazards, where American interests, aspirations, and way of life can thrive.

As the threats and hazards we face change, the way we and our partners and stakeholders carry out our missions must change as well. The second Quadrennial Homeland Security Review comprehensively examined the homeland security strategic environment and identified strategic shifts and areas of ongoing priority and renewed emphasis for the Nation’s long-term homeland security strategy.

To set homeland security priorities, DHS leads national efforts to assess, analyze, and compare risk—which is a function of the likelihood and potential impacts of different homeland security threats and hazards. However, we recognize that the likelihood and consequence of specific threats and hazards may be influenced over time by interdependent economic, political, social, environmental, and technological factors, as well as trends and future uncertainties. We use systems analysis to create a more dynamic view of how these forces influence threats and hazards and how risk may change over time. This forward-looking understanding of risk allows us to prioritize our actions within the five missions and maximize the use of our limited resources.
Based on a deep examination of the strategic environment, we identified six drivers of change and six challenges that pose the most strategically significant risk over the next five years (described in the Strategic Environment section). From those drivers and challenges, we identified the following strategic priorities that impact all five homeland security missions:

- An updated posture to address the increasingly decentralized terrorist threat;
- A strengthened path forward for cybersecurity that acknowledges the increasing interdependencies among critical systems and networks;
- A homeland security strategy to manage the urgent and growing risk of biological threats and hazards;
- A risk segmentation approach to securing and managing flows of people and goods into and out of the United States; and
- A new framework for improving the efficiency and effectiveness of our mission execution through public-private partnerships.

Beyond these strategic priorities, this second quadrennial review also highlights ongoing areas of priority and renewed areas of emphasis based on risk and other considerations—countering nuclear threats, strengthening our immigration system, and enhancing national resilience. Finally, building upon the first Quadrennial Homeland Security Review, this review provides an updated view of the Nation’s homeland security mission goals and objectives.
3. THE STRATEGIC ENVIRONMENT

DRIVERS OF CHANGE

This Nation’s homeland security architecture has matured over the past four years, as illustrated by the development of a One DHS approach to a range of homeland security challenges, and we are determined that this progress continue. For example, programs such as TSA Pre✓™ and Global Entry demonstrate the effectiveness and efficiency of risk-based security and cross-Departmental integration that can be achieved within budget constraints. In addition, law enforcement is becoming increasingly adept at identifying and disrupting terrorist plotting in this country. It is also worth noting that, in late 2013, DHS received its first unqualified or “clean” audit opinion; this occurred just 10 years after the Department’s formation, which was the largest realignment and consolidation of federal government agencies and functions since the creation of the Department of Defense in 1947.

Our charge in the quadrennial review, however, is to identify and describe the threats to the
The first step in understanding threats and hazards is identifying key areas of change. These areas of change are detailed below.

THE EVOLVING TERRORISM THREAT

The nature of the terrorist threat to the United States has evolved since the September 11, 2001 attacks—and indeed, since the first Quadrennial Homeland Security Review in 2010. Counterterrorism pressure in the Afghanistan–Pakistan region has degraded the ability of al-Qa’ida’s senior leadership to launch sophisticated external attacks, although the leadership that remains continues to aspire to attack the United States. At the same time, other groups affiliated and ideologically aligned with al-Qa’ida have emerged with the intent and, in some cases, the capability to carry out attacks against the United States and American citizens overseas.

Al-Qa’ida in the Arabian Peninsula is currently the al-Qa’ida affiliate of the greatest concern because of its demonstrated and continuing interest in advancing plots to attack the United States, particularly against the aviation industry.

Also of concern are militants who support al-Qa’ida’s international agenda and have established bases of operation in conflict zones in the Middle East, West Africa, and North Africa, particularly in Syria and neighboring states. These safe havens could allow them to plan and launch external operations and train recruits who have Western passports and who can return home with combat skills and a violent anti-Western agenda.

Al-Qa’ida, its affiliates, and adherents also use propaganda to inspire U.S.- and Western-based supporters who have not traveled to conflict zones to conduct terrorist attacks. Lone offenders—prime targets of English-language messaging by al-Qa’ida affiliates—tend to favor plots involving the use of easily acquired weapons or explosives. Lone offenders and small groups acting on their own initiative and without direction of a terrorist group are among the most persistent and difficult threats to counter. In recent years, there have been several acts of violence against military targets by lone offenders as well as attempted attacks on civilian populations by individuals motivated by al-Qa’ida. In addition, other groups and individuals inspired by a range of religious, political, or other ideological beliefs have promoted and used violence against the United States. While not as...
significant as the threat posed by al-Qa’ida, its adherents, and its affiliates, these other
groups and individuals remain a persistent threat.

Improvised explosive devices continue to represent a significant threat because they are
easy to build and popular among violent extremists. Further, violent extremists have shown
an enduring interest in improving improvised explosive device materials and methods to
evade security measures. Violent extremists also seek to conduct small arms attacks.
While violent extremists’ mistakes have sometimes contributed to intelligence and law
enforcement successes, plots using improvised explosive devices or small arms present
unique challenges as a result of being tactically simple and adaptable in both timing and
location of execution, complicating discovery and disruption by authorities.

Chemical, biological, radiological, and nuclear threats are enduring areas of concern; the
consequences of these attacks are potentially high even though the likelihood of their
occurrence is relatively low. Small scale chemical attacks are expected to remain more
likely, because of accessibility to precursor materials and toxic industrial chemicals and the
relative lack of specialized skills and knowledge required to conduct such attacks.
However, nuclear terrorism and bioterrorism pose the most strategically significant risk, the
former because of its potential consequences, and the latter because of potential
increases in both likelihood and consequence. While the difficulty of stealing a nuclear
weapon or fabricating one from stolen or diverted weapons materials reduces the
likelihood of this type of attack, the extremely high consequences of an improvised nuclear
device attack make it an ongoing top homeland security risk. Biological terrorism becomes
more likely as the capability, knowledge, and resources required to carry out an attack
become more widely accessible. While biotechnology has great potential for good, its
continued expansion around the world challenges our ability to prevent and detect
potential bioterrorist incidents.

INFORMATION AND COMMUNICATIONS TECHNOLOGY

The globally interconnected digital information and communications infrastructure, known
as cyberspace, has changed dramatically in recent years. Cyberspace has become an
integral part of daily life in America and around the world. An estimated two billion people
have at least 12 billion computers and devices, including global positioning systems,
mobile phones, satellites, data routers, desktop computers, and industrial control
computers that run power plants, water systems, and more. A vast array of interdependent
information technology networks, systems, services, and resources enable communication,
facilitate travel, power our homes, run our economy, and provide essential government
services. These systems provide enormous benefits to our society and economy, but they also create new risks and vulnerabilities.

Malicious actors continue to become more sophisticated in exploiting these vulnerabilities, increasing the risks to critical infrastructure. These actors seek to steal financial information, intellectual property, trade secrets, and other sensitive information from businesses small and large. They also seek to capture personal and financial information from our citizens. While many corporations make cybersecurity a core aspect of their enterprise risk management, many small businesses and public sector entities face financial and personnel constraints in doing the same.

At the same time, information and communications technology are enabling goods and services to flow through the global supply chain more rapidly than ever before. Moreover, flows of data and information are, in some cases, replacing physical flows of goods. One example of this dynamic is the emerging trend of three-dimensional printing. Of concern, the ongoing development and adoption of electronic payment systems and their increasing use for illicit trafficking and smuggling create substantial new challenges for investigation and interdiction.
We must not forget that cyberspace provides opportunities for homeland security. With appropriate protections for individual privacy and civil rights and civil liberties, technology can enhance situational awareness, improve investigative capabilities, and support operational integration.

**NATURAL DISASTERS, PANDEMICS, AND CLIMATE CHANGE**

Natural disasters, pandemics, and the trends associated with climate change continue to present a major area of homeland security risk.

Of the naturally occurring events, a devastating pandemic remains the highest homeland security risk. Both the likelihood and consequences of this low probability, high-impact event are expected to increase, driven in large part by increasing opportunities for novel infectious diseases to emerge and spread quickly around the world. Changes in land use and agriculture, including rising urbanization in countries where disease is endemic or potentially endemic, promote the emergence of potential pandemic-causing diseases. Increasing global trade and travel have the potential to fuel the spread of infectious diseases around the world, challenging the capacity of public health systems at home and abroad to handle pandemics. Rising antiviral and antibacterial resistance have the potential to severely limit the effectiveness of available medical countermeasures, but other disease prevention and treatment techniques are now emerging.

Weather events present a significant and growing challenge, with several multi-billion dollar disasters in recent years. Hurricane Sandy, the largest diameter Atlantic storm on record, is estimated to have killed 117 people in the United States and caused widespread flooding. More than 8.5 million people were left without power, and the storm caused tens of billions of dollars in damage. Other disasters, particularly earthquakes, droughts, and floods, also pose significant risks to the Nation. The risk of these disasters is increased by the vulnerability of aging infrastructure, increasing population density in high-risk areas,
and—in the case of droughts, floods, and hurricanes—by trends associated with climate change. Pandemic disease, hurricanes, and other natural disasters not only have the potential to cause severe consequences, including fatalities and economic loss, but also may overwhelm the capacities of critical infrastructure, causing widespread disruption of essential services across the country.

Climate change and associated trends may also indirectly act as “threat multipliers.” They aggravate stressors abroad that can enable terrorist activity and violence, such as poverty, environmental degradation, and social tensions. More severe droughts and tropical storms, especially in Mexico, Central America, and the Caribbean, could also increase population movements, both legal and illegal, across the U.S. border. Melting sea ice in the Arctic may lead to new opportunities for shipping, tourism, and legal resource exploration, as well as new routes for smuggling and trafficking, increased risk of environmental disasters, and illicit resource exploitation. Higher temperatures may change patterns of human, animal, and plant diseases, putting the workforce, the general public, and plant and animal health at higher risk of illness. The United States may need to prepare for more frequent, short-term, disaster-driven migration. Higher temperatures and more intense storms may also damage or disrupt telecommunications and power systems, creating challenges for telecommunications infrastructure, emergency communications, and the availability of cyber systems. Finally, the cost of preparing for, responding to, and recovering from such events is anticipated to grow as weather-related events continue to become more severe and damaging.
INTERDEPENDENT AND AGING CRITICAL INFRASTRUCTURE SYSTEMS AND NETWORKS

The Nation’s critical infrastructure provides the essential services that underpin the American way of life. The concept of critical infrastructure as discrete, physical assets has become outdated as everything becomes linked to cyberspace. This “cyber-physical convergence” has changed the risks to critical infrastructure in sectors ranging from energy and transportation to agriculture and healthcare. Moreover, this interconnected cyber-physical infrastructure consists of multiple systems that rely on one another to greater degrees for their operations and, at times, operate independent of human direction. One example of this type of interconnected system is the global supply chain, where information and communications technologies are providing real-time location services, traffic updates, emergency notifications, and more.

Critical infrastructure owners and operators also continue to experience increasingly sophisticated cyber intrusions, which provide malicious actors the ability to disrupt the delivery of essential services, cause physical damage to critical infrastructure assets, and potentially produce severe cascading effects.

The aging or deteriorating condition of significant aspects of critical infrastructure systems weakens our resilience and can affect our Nation’s security and prosperity. Infrastructure investment has not kept pace with U.S. population growth or growth in demand. One-third of major roads are in poor or mediocre condition, and approximately one-quarter of the Nation’s bridges are either structurally deficient or functionally obsolete. Though growth in demand for electricity has slowed, funding gaps for electric infrastructure could top $100 billion by the end of the decade. Overall, blackouts and other electrical disturbances have increased by more than 140 percent since 2007. Although weather-related events have
been the main cause of major electrical outages in the United States, many outages have been attributed to system operations failures, and reliability issues are emerging due to the complex issues of retiring older infrastructure. Without investment in recapitalization and new technologies, and in light of the potential for increased weather events, the aging electric grid will likely continue to experience disruptions in service. Our country needs an estimated $682 billion in wastewater and drinking water infrastructure improvements over the next 20 years, as well. Hurricane Sandy caused an estimated combined 11 billion gallons of sewer overflows in eight northeast states and the District of Columbia.

Due in large part to financial constraints, the Nation’s public health capacity has eroded in recent years, as inadequate funding for infrastructure—from laboratories to community health centers—has been aggravated by increased demand on an already strained system. As a result, public health infrastructure systems are under significant strain on a day-to-day basis, leading to decreased capacity to address large-scale public health emergencies that may emerge.

These challenges present significant obstacles to performing our missions, particularly during times of disaster. However, there are unique opportunities to build our critical infrastructure systems to be more reliable, efficient, and resilient than they were before. For example, as we rebuild aging and failing infrastructure, we can design in cost-effective security and resilience features. By leveraging new tools, such as information and communications technology, building stronger partnerships, and adopting key lessons learned, we are able to update and adapt critical infrastructure systems to better meet future challenges.

FLOWS OF PEOPLE AND GOODS: INCREASING VOLUME AND SPEED

Flows of people and goods around the world have expanded dramatically in recent years. The value of U.S. exports and imports increased substantially between 2005 and 2012; exports increased by 72 percent, and imports increased by 36 percent. Both are expected to grow an average of six percent annually through 2030. Lawful travel to the United States increased 36 percent from 2005 to 2012 and is estimated to increase by more than 25 percent from 2012 to 2018. Air travel has also seen substantial growth internationally, increasing by 47 percent in the same seven-year period.

These trends will be amplified by other factors, including the forthcoming expansion of the Panama Canal, which is likely to substantially increase the volume of trade going through U.S. ports on the East Coast and in the Gulf of Mexico. In addition, the global systems that move goods from one location to another have grown increasingly efficient through
Figure 2: Lawful travel to the United States increased 36 percent from 2005 to 2012 and is estimated to increase by more than 26 percent from 2012 to 2018.

innovations such as intermodal shipping. This has increased trade over our borders. Rail intermodal traffic—transporting shipping containers and truck trailers on railroad flat cars—increased nearly fourfold between 1980 and 2012.

However, the trade and travel system is also susceptible to threats and hazards. When air and maritime travel into and within the United States was halted in the immediate aftermath of the attacks of September 11, 2001, the resulting disruptions had tremendous negative impacts on our economy. Short-term supply chain disruptions due to port strikes and natural disasters have also impacted flows of cargo. Cascading events, such as the 2011 earthquake and tsunami in Japan that led to the Fukushima Daiichi nuclear disaster and the temporary idling of auto plants in the United States, demonstrate the potential for significant disruption to the lawful trade and travel system.

The increased movement of people and goods across our borders provides many opportunities but also provides more places for illegal goods, unauthorized migrants, and
threats to hide. Illicit materials, threats, and hazards may cross at or between our ports of entry deliberately or inadvertently. Illegal shipments, such as intellectual property infringing goods, adversely impact our nation’s economy. Unauthorized migration is influenced by many factors, including weak rule of law and violence in sending countries. Violent extremists and criminals can hide within this larger flow of migrants who intend no harm. More travelers moving more efficiently through the lawful trade and travel system also may increase the potential for rapid escalation of biological events across regions, countries, and continents.

Transnational criminal organizations rely on revenues generated through the sale of illegal drugs and counterfeit goods, human trafficking and smuggling, and other criminal activities. These organizations continue to expand in size, scope, and influence and are capitalizing on technological innovation, including new platforms to sell illicit goods, innovative ways of moving money, tools for coordinating operations, and a variety of other criminal and cyber activities. Transnational criminal organizations are gaining strength by taking advantage of the same innovations in management and supply chain structures that are propelling multinational corporations.

As transnational criminal organizations grow stronger and challenge or corrupt governments in many regions, they are moving more freely, expanding their networks, and acquiring and distributing military-grade equipment. Violent extremist networks can also conduct these profitable criminal activities on their own, exploiting the same vulnerabilities in finance, trade and travel, and immigration.

Generally, higher volumes of people and goods will stress current screening and detection capabilities and capacities.

**BUDGET DRIVERS**

The out year funding assumptions applied for this quadrennial review are based on the economic and policy assumptions underpinning the President’s 2015 Budget submission to Congress. Since the last Quadrennial Homeland Security Review, economic conditions have had wide-ranging impacts across homeland security partners and stakeholders, affecting both daily operations and current investments to meet longer-term needs and challenges. For example, more than two-thirds of the nation’s 30 largest metro regions have not seen municipal government revenue return to pre-recession levels. While public safety spending is often the last part of the budget to be cut, by 2011, 20 of the 30 largest metro regions had reduced spending on public safety, impacting daily operations and the ability to respond to emergencies.
Going forward, the budgets of many homeland security partners are assumed to maintain parity with inflation or modestly decline in real terms. We also assume that state budgets will be constrained by reductions in federal grants, which are projected to remain below their 2007 historic high (as a percentage of gross domestic product). International partners will likely face similar constraints. Economic pressures on families, nonprofits, and the private sector may also adversely affect local investment in the security and resilience of our communities.

Partnerships with state, local, tribal, and territorial governments; international partners; nongovernmental organizations; and the private sector are essential to meet mutual safety and security needs and extend services in a time of flat or declining budgets. State, local, tribal, and territorial governments are maintaining services through measures such as sharing resources across jurisdictional lines and privatizing infrastructure. Public-private partnerships are a key focus of this report because the security challenges facing our Nation are too large and complex for either government or the private sector to address alone. Working together to invest in infrastructure projects and to expedite travel and trade benefits both private and public sectors.
PREVAILING CHALLENGES THAT POSE THE MOST STRATEGICALLY SIGNIFICANT RISK

The threats, hazards, trends, and other dynamics reflected in the drivers of change suggest several prevailing strategic challenges that will drive risk over the next five years:

- The **terrorist threat** is evolving and, while changing in shape, remains significant as attack planning and operations become more decentralized. The United States and its interests, particularly in the transportation sector, remain persistent targets.

- Growing **cyber threats** are significantly increasing risk to critical infrastructure and to the greater U.S. economy.

- **Biological concerns** as a whole, including bioterrorism, pandemics, foreign animal diseases, and other agricultural concerns, endure as a top homeland security risk because of both potential likelihood and impacts.

- **Nuclear terrorism** through the introduction and use of an improvised nuclear device, while unlikely, remains an enduring risk because of its potential consequences.

- **Transnational criminal organizations** are increasing in strength and capability, driving risk in counterfeit goods, human trafficking, illicit drugs, and other illegal flows of people and goods.

- **Natural hazards** are becoming more costly to address, with increasingly variable consequences due in part to drivers such as climate change and interdependent and aging infrastructure.

Beyond these specific strategic challenges, factors such as technology and migration present both opportunities and challenges for the homeland security community. Technological advances in communications, big data, manufacturing, and biological sciences provide new and lower cost capabilities that may benefit both the United States and our adversaries. Similarly, while lawful immigration greatly benefits the United States, attempted unauthorized migration poses consistent challenges for the management of our legal immigration system, borders, and ports of entry.
POTENTIAL “BLACK SWANS”

There are potential changes in the world around us that, while highly unlikely, would dramatically impact homeland security were they to occur. Such changes may come from previously unknown aspects of the strategic environment or may be the result of known aspects behaving in an unforeseen and unpredictable manner and have been referred to by economists and sociologists as “black swans.”

While not an exhaustive list, there are four potential “black swans” that could materially change our assessment of overall homeland security risk and priorities over the next five years:

- Rapid adoption of technology-driven changes to manufacturing processes, such as three-dimensional printing, fundamentally altering the importance of transnational flows of information in relation to the transnational flows of goods;

- A country unexpectedly becoming a failed state, leading to consequences such as loss of control over sensitive technologies (e.g., chemical, biological, radiological, and nuclear materials) or loss of general border integrity;

- A substantial increase in sophistication of hostile non-state actors, such as a violent extremist group gaining the ability to launch a campaign of well-coordinated and highly organized attacks, conducted by interconnected but autonomous groups or individuals within the United States; and

- Abrupt impacts of climate change, such as drastic alterations in U.S. weather patterns and growing seasons or rapid opening of the Arctic.

These changes are not planned for or expected in the next five years, yet if they were to happen, they would fundamentally alter the homeland security strategic environment described here.
4. GUIDING PRINCIPLES

The following principles form the basis for the specific priorities and areas of emphasis the Department, together with our partners and stakeholders, will adopt in addressing the strategic challenges discussed in the Strategic Environment section.

THE CORNERSTONE OF HOMELAND SECURITY IS PREVENTING TERRORISM, BUT HOMELAND SECURITY MUST BE MULTI-THREAT AND ALL-HAZARD

Events of the past 12 years demonstrate that we must consider the full range of threats and hazards facing the Nation when setting homeland security strategy and priorities. The Department is a multi-mission, multi-function agency, covering long-standing functions such as civil defense, emergency response, customs, border control, law enforcement, and immigration. As one agency, we are able to improve efficiency by identifying the common characteristics among the wide variety of threats and hazards we face and by identifying common ways to address them.
HOMELAND SECURITY SUPPORTS ECONOMIC SECURITY

As noted previously, lawful trade and travel are expanding rapidly, with great benefit to U.S. prosperity and economic security. DHS and our partners are on the front lines overseas and at our air, land, and sea ports of entry, expediting these flows of people and goods and ensuring their security. As such, and as recognized in successive national security strategies, homeland security is inseparable from economic security.

HOMELAND SECURITY REQUIRES A NETWORKED COMMUNITY

The Department works with other units of government, forms public-private partnerships, and enlists the help of the American people because the homeland security missions cannot be met by one entity alone. Our ability to effectively network ourselves through robust partnerships and operational integration—within DHS, across homeland security partners and stakeholders, and with our international partners—increasingly means the difference between mission success and failure. This is all the more important given the range of adversaries the Nation confronts, many of whom are increasingly networked themselves. The homeland security community can be more flexible, adaptable, and efficient in addressing diverse challenges if it acts as an integrated, mutually supporting network. Our shared efforts will promote security and risk reduction approaches that are responsive to the needs of our partners.

HOMELAND SECURITY RELIES UPON THE USE OF MARKET-DRIVEN SOLUTIONS AND INNOVATION

We must partner with industry in research and development efforts to reduce known vulnerabilities that have proven difficult or expensive to address—particularly in cyberspace.
and critical infrastructure—and to mitigate consequences of disruption or intrusion. The Department will continue to adopt market-based solutions and coordinate closely with industry to identify new areas of application for security products and services and will help ensure the public and private sectors have awareness and access to the latest technologies and protections.

HOMELAND SECURITY UPHOLDS PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES

Privacy, civil rights, and civil liberties issues are interwoven into our approach to homeland security across all missions and can arise in any homeland security activity, sometimes in unforeseen ways. In addressing new risks or adopting new and integrated approaches, we must identify early on any risk of infringement of these core values and rights and address that risk accordingly. When issues are identified and resolved earlier, it helps ensure that all eligible persons and communities can participate in homeland security programs and benefit from our operations.

HOMELAND SECURITY IS NATIONAL RISK MANAGEMENT

Absolute security against the threats and hazards we face is neither fiscally nor operationally possible. Instead, homeland security is about managing risk. As described previously, the second quadrennial review makes recommendations for strategic shifts and renewed areas of emphasis for our national homeland security strategy and priorities. National risk management emphasizes focusing on those actions and interventions that reduce the greatest amount of strategic risk to the Nation.
5. STRATEGIC PRIORITIES

DHS will adopt the following strategic shifts or renewed emphases over the next four years to best address the changing strategic environment. These priorities emerge out of a number of cross-cutting Quadrennial Homeland Security Review studies, which lead to shifts and renewed areas of emphasis across the homeland security missions. The tables at the beginning of each subsection below show which missions are impacted by these shifts and renewed areas of emphasis.

SECURING AGAINST THE EVOLVING TERRORISM THREAT

OVERVIEW

As described in the first quadrennial review, homeland security is a concerted national effort that involves actions by a widely distributed and diverse group of federal, state, local, tribal, territorial, non-governmental, and private sector partners as well as individuals, families, and communities. The evolution of the terrorist threat demands a well-informed, highly agile, and well-networked group of partners and stakeholders to anticipate, detect,
target, and disrupt threats that challenge national security, economic prosperity, and public safety. To improve overall unity of effort, we will work with our partners to identify, investigate, and interdict legitimate threats as early as possible; expand risk-based security; focus on countering violent extremism and helping to prevent complex mass casualty attacks; reduce vulnerabilities by denying resources and targets; and uncover patterns and faint signals through enhanced data integration and analysis.

Table 1: The following table shows how priority areas of emphasis for securing against the evolving terrorism threat map to the homeland security missions.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify, Investigate, and Interdict Threats as Early as Possible</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shrink the Haystack: Expand Risk Based Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Focus on Countering Violent Extremism and Helping to Prevent Complex Mass Casualty Attacks</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduce Vulnerabilities: Deny Resources, Deny Targets</td>
<td>✔</td>
<td></td>
<td></td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Uncover Patterns and Faint Signals: Enhance Data Integration and Analysis</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**STRATEGIC APPROACH**

**IDENTIFY, INVESTIGATE, AND INTERDICT THREATS AS EARLY AS POSSIBLE**

Given the current and emerging potential threats, a primary concern is that violent extremists can move undetected across porous borders within conflict zones—such as today’s conflicts in Syria, Somalia, and Yemen—where they can train in terrorist tactics, skills, and weapons. At the same time, several countries are on the edge of state failure and are unable to secure their own borders, prevent the illicit movement of people and goods, and collect customs revenues to support governance.

To address these pathway vulnerabilities and enhance the safe and secure movement of people and goods, DHS, in coordination with the Departments of State, Defense, Justice, and other partners, will prioritize support to foreign partners to increase their border
management, customs integrity, and law enforcement capabilities and capacities. In addition, we will continue to expand pre-departure screening and enhance transportation security operations among willing partners to mitigate risks from overseas. To keep dangerous people and goods off aircraft bound for the United States, it is critical that we use information received in advance to screen abroad based on risk, rather than waiting for arrival in the United States.

**SHRINK THE HAYSTACK: EXPAND RISK-BASED SECURITY**

The decentralized nature of today’s threat demands that we continue to move away from one-size-fits-all security approaches and toward risk-informed, intelligence-driven approaches. For this reason, DHS will expand efforts to identify low-risk travelers and cargo to focus security resources on those we know less about or those identified as higher risk. Trusted traveler and shipper programs such as Global Entry, TSA Pre✓™, and the Customs-Trade Partnership Against Terrorism advance these objectives and show that effective security and the expedited flow of goods and people can be achieved together. We will continue to identify lower-risk travelers by a number of means, including using background checks and recognizing foreign partner trusted traveler and shipper programs.

More broadly, risk-informed decision making is becoming the norm among homeland security partners and stakeholders. For example, unmanned aerial surveillance systems
The strategic priorities outlined in the text focus on securing and managing borders, using risk-based deployments of security teams, improving approaches to insider threats, and enhancing security in mass transit and other transportation modes. The text also highlights efforts to counter violent extremism, emphasizing local communities and community-oriented policing efforts. Furthermore, the document notes the ongoing research and analysis to identify tactics, behaviors, and indicators associated with violent extremism. DHS is working with partners to share information about Internet-based radicalization and to train law enforcement officers on behaviors indicative of violent extremist activity.
Similar research into non-ideologically motivated violence, such as the devastating shootings in Newtown, Connecticut and Aurora, Colorado, provides further insight into pre-incident behavioral indicators associated with mass violence. These insights enhance our efforts to equip partners with the most effective tools to identify and mitigate a range of violent attacks, including briefings to community stakeholders on pre-incident behavioral indicators associated with mass casualty shootings and on community-based multidisciplinary intervention techniques.

**REDUCE VULNERABILITIES: DENY RESOURCES, DENY TARGETS**

Violent extremists will seek to attack symbolic venues, transportation pathways, mass gatherings, and critical infrastructure. To enhance our ability to protect these “soft” targets, we must adopt approaches that are intelligence-led, analytically driven, and pursued in close cooperation between federal, state, local, tribal, territorial, and private sector partners as well as with the public. The DHS “Security Strategy for Mass Transit and Passenger Rail” illustrates how we have employed this approach to improve the security and resilience of critical surface transportation infrastructure.

Further, to counter the threat posed by improvised explosive devices and small arms attacks, we will work with our partners to expand and promote activities such as suspicious activity reporting and private sector security measures. Internationally, we will continue to support multilateral efforts, such as the World Customs Organization’s Program Global
Shield, which shares information on the global movement of precursor chemicals used to manufacture improvised explosive devices and raise security standards. We regulate high-risk chemical facilities to reduce their vulnerabilities. We will also continue researching next-generation technology solutions to stay ahead of advances in wireless technology, given the use of wireless technology in improvised explosive device detonation and control mechanisms.

Across all of these efforts, DHS, working with our government and private sector partners, will be proactive in discouraging terrorist plots. We will place an increased emphasis on deterrence, including enhancing efforts to publicly communicate tailored descriptions of homeland security capabilities to influence the perceptions, risk calculations, and behaviors of adversaries.

**UNCOVER PATTERNS AND FAINT SIGNALS: ENHANCE DATA INTEGRATION AND ANALYSIS**

DHS and our partners must continually enhance situational awareness. To that end, DHS is committed to integrating its data sources, including by consolidating or federating screening and vetting operations. Perhaps most importantly, we must continually improve our ability to make sense of vast amounts of intelligence and other information—the so-called “big data” challenge—while rigorously protecting the privacy and civil liberties of Americans. For homeland security, the adoption of big data management solutions will aid investigators and analysts in identifying relationships that were previously difficult to discern. This type of pattern and network analysis allows DHS and our partners to identify harmful activity as early as possible and to take steps to intervene or otherwise stop harmful events from occurring.

One critical data source is Suspicious Activity Reporting from state, local, tribal, territorial, and private sector partners as part of the Nationwide Suspicious Activity Reporting Initiative. Another source is the “If You See Something, Say Something™” campaign, which encourages citizens to report suspicious activity to the proper law enforcement authorities. These efforts ensure the protection of privacy, civil rights, and civil liberties, while also ensuring information is quickly reviewed by the Federal Bureau of Investigation’s (FBI’s) Joint Terrorism Task Forces for possible investigation and shared with other fusion centers and FBI Field Intelligence Groups for additional analysis. Through the National Network of Fusion Centers and other mechanisms, DHS will prioritize the development and timely distribution of locally or regionally oriented joint products. These joint products, produced collaboratively by federal, state, local, tribal, and territorial partners, support operations and provide detailed insight on emerging community or region-specific threats.
SAFEGUARD AND SECURE CYBERSPACE

OVERVIEW

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. A range of traditional crimes is now being perpetrated through cyberspace. This includes the production and distribution of child pornography and child exploitation conspiracies, banking and financial fraud, intellectual property violations, and other crimes, all of which have substantial human and economic consequences.

Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks.
Of growing concern is the cyber threat to critical infrastructure. This infrastructure provides essential services such as energy, telecommunications, water, transportation, and financial services and is increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend.

In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission. The Department works to achieve this mission by collaborating with government and private sector partners to strengthen cybersecurity protections, investigate those that engage in cybercrime, and take full advantage of innovations in machine intelligence and communications that work at the speed of cyberspace. The Department will promote security and risk reduction approaches that are driven by the needs of our stakeholders, are cost effective, and do not negatively impact operational performance. When incidents do occur, DHS will continue to provide assistance to potentially impacted entities, analyze the potential impact across critical infrastructure, investigate those responsible in conjunction with other law enforcement partners, and coordinate the national response to significant cyber incidents.

The Department works in close coordination with other agencies with complementary cyber missions, as well as private sector and other nonfederal owners and operators of critical infrastructure, to ensure greater unity of effort and a whole-of-nation response to cyber incidents. DHS coordinates the national protection against, mitigation of, and recovery from cyber incidents; works to prevent and protect against risks to critical infrastructure; disseminates domestic cyber threat and vulnerability analysis across critical infrastructure sectors; secures federal civilian systems; investigates, attributes, and disrupts cybercrimes under its jurisdiction; and coordinates federal government responses to significant incidents, whether cyber or physical, affecting critical infrastructure. The Department of Justice (DOJ) prosecutes cybercrimes; investigates, attributes, and disrupts cybercrimes under its jurisdiction; leads domestic national security operations regarding cyber threats, including disrupting foreign intelligence, terrorist, or other national security threats; and conducts domestic collection, analysis, and dissemination of cyber threat information. The Department of Defense (DOD) defends the nation from attack, secures national security and military systems, and gathers foreign cyber threat information. Working together, we work to foster a secure and resilient cyberspace that protects privacy and other civil liberties by design; supports innovation and economic growth; helps maintain national
security and public health and safety; and supports legitimate commerce.

Table 2: The following table shows how priority areas of emphasis for safeguarding and securing cyberspace map to the homeland security missions.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Strengthen the Security and Resilience of Critical Infrastructure</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Secure the Federal Civilian Government Information Technology Enterprise</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Advance Law Enforcement, Incident Response, and Reporting Capabilities</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strengthen the Ecosystem</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

### STRATEGIC APPROACH

**STRENGTHEN THE SECURITY AND RESILIENCE OF CRITICAL INFRASTRUCTURE**

The Department employs a risk-informed approach to safeguarding critical infrastructure in cyberspace. We do this in the context of the overall risk to critical infrastructure under an all-hazards approach. In reducing cyber and physical risks, we will emphasize protections for privacy and civil liberties, transparent and accessible security processes, and domestic and international partnerships that further collective action. The Department will continue to coordinate with sector specific agencies, other federal agencies, and private sector partners to share information on and analysis of cyber threats and vulnerabilities and to understand more fully the interdependency of infrastructure systems nationwide. This collective approach to prevent, protect against, mitigate, respond to, investigate, and recover from cyber incidents prioritizes understanding and meeting the needs of our partners. This approach is also consistent with the growing recognition among corporate leaders that cyber and physical security are interdependent and must be core aspects of their risk management strategies.

The Department will evolve towards dynamic real-time situational awareness capabilities, like “weather maps” for cyberspace. These situational awareness capabilities will support cyber infrastructure that—much like the human immune system—will be smart enough to
detect, adapt to, and defend against new threats with sufficient resilience to continue operating while under attack. Further, this situational awareness will support a common operating picture for cybersecurity that will provide cyber event information, and serve as a resource for all of government and industry. Providing information to machines at machine speed to block threats in milliseconds instead of the hours or days required today will enable better cyber incident response and mitigation.

We must draw on the Nation’s full range of expertise and resources—from all levels of government, the private sector, members of the public, and international partners—to secure critical infrastructure from cyber threats. Executive Order 13636, Improving Critical Infrastructure Cybersecurity (2013), and Presidential Policy Directive 21, “Critical Infrastructure Security and Resilience” (2013), establish a risk-informed approach and a framework for critical infrastructure security and resilience collaboration. They also include the Framework for Improving Critical Infrastructure Cybersecurity, which provides an industry-driven risk management approach to strengthen cybersecurity across all critical infrastructure sectors. We will continue to work with our partners to foster development of secure cyber products and services and to encourage the adoption of leading cybersecurity best practices, including the Cybersecurity Framework and the National Infrastructure Protection Plan. The cyber ecosystem will also be strengthened as aging and failing infrastructure is replaced by infrastructure with more secure and resilient design built in.

**Secure the Federal Civilian Government Information Technology Enterprise**

The Federal Government must seek to serve as a model to other organizations in our work to secure our networks with the latest tools, information, and protections. The Department
will continue to work with each federal civilian department and agency to promote the adoption of common policies and best practices that are risk-based and able to effectively respond to the pace of ever changing threats. As systems are protected, alerts can be issued at machine speed when events are detected to help protect networks across the government information technology enterprise and the private sector. This enterprise approach will help transform the way federal civilian agencies manage cyber networks through strategically sourced tools and services that enhance the speed and cost-effectiveness of federal cybersecurity procurements and allow consistent application of best practices.

The Department works with other federal agencies and the private sector to identify emerging requirements and to support research and development projects that keep pace with ever changing threats and vulnerabilities. The Department will target techniques and capabilities that can be deployed over the next decade with the potential to redefine the state of cybersecurity against current and future threats by working to make the innovations from research and development widely available across the public and private sectors.

**Advance Law Enforcement, Incident Response, and Reporting Capabilities**

Complementary cybersecurity and law enforcement capabilities are critical to safeguarding and securing cyberspace. Law enforcement performs an essential role in achieving our Nation’s cybersecurity objectives by investigating a wide range of cybercrimes, from theft...
and fraud to child exploitation, and apprehending and prosecuting those responsible. Cybersecurity and infrastructure protection experts provide assistance to owners and operators of critical systems by responding to incidents and restoring services, and analyzing potentially broader cyber or physical impacts to critical infrastructure.

Law enforcement entities; network security experts; the Intelligence Community; state, local, tribal, and territorial partners; critical infrastructure owners and operators; and others in the private sector, through coordination and planning, will increase the quantity and impact of cybercrime investigations and network security efforts. Together we will continue to identify and respond to malicious actors and continue to grow our national cyber incident response and information sharing capacity. We will also continue sharing lessons learned from these efforts to help prevent the same incidents from happening elsewhere, while protecting victims’ privacy and ongoing investigations.

Criminal investigators and network security experts with deep understanding of the technologies malicious actors are using and the specific vulnerabilities they are targeting work to effectively respond to and investigate cyber incidents. DHS will work with other federal agencies to conduct high-impact criminal investigations to disrupt and defeat cyber criminals, prioritize the recruitment and training of technical experts, develop standardized
methods, and broadly share cyber response best practices and tools. The Secretary of Homeland Security will coordinate federal government responses to significant cyber or physical incidents affecting critical infrastructure consistent with statutory authorities.

DHS will continue to work with all partners, government and private sector, to ensure that information provided to any federal agency is appropriately shared. This strengthens the use of established private sector and academia relationships with government partners and leverages these relationships when they are needed most.

**STRENGTHEN THE ECOSYSTEM**

Cybersecurity is a shared responsibility in which each of us has a role. Ensuring a healthy cyber ecosystem will require collaborative communities, innovative and agile security solutions, standardized and consistent processes to share information and best practices, sound policies and plans, and development of a skilled workforce to ensure those policies and plans are implemented as intended.

DHS will work with our public and private sector partners to help develop innovative security technologies and services that strengthen analytic, response, and remediation capabilities; prevent incidents before they occur; and minimize the consequences of those incidents that occur. To do this, we will develop a strong team of cybersecurity professionals to design, build, and operate robust technology to reduce exploitable weaknesses.

The cyber ecosystem also needs self-mitigating and self-healing systems to address threats at machine speed. Consistent standards are needed for sharing information across organizations and developing interoperable technologies that enable detection of and resilience against threats and hazards. DHS will work with our public and private sector partners and across the science and policy communities to identify promising technologies, policies, and standards that enable trust-based, privacy-centric, automated sharing of cybersecurity information to limit the spread of incidents and minimize consequences.

DHS will continue to advance existing public education programs and promote cybersecurity strategies and awareness campaigns that engage the American people in keeping themselves—and the Nation—secure online. Internationally, DHS will work with the Department of State and other partners to build global networks to share vital cybersecurity information and help enable international response to cyber incidents. DHS, with our partners, will also work to harmonize international laws to effectively combat transnational cybercrime.
A HOMELAND SECURITY STRATEGY FOR COUNTERING BIOLOGICAL THREATS AND HAZARDS

OVERVIEW

Biological threats and hazards—ranging from bioterrorism to naturally occurring pandemics—are a top homeland security risk. They have the potential to significantly impact the health and well-being of the Nation’s people, animals, and plants. These threats and hazards may also be highly disruptive to our efforts to pursue the homeland security missions. They may overwhelm our state, local, tribal, and territorial partners and may threaten our ability to maintain essential functions and carry out day-to-day operations.

We generally expect the risk of biological threats and hazards to increase over time, given trends such as increasing trade and travel and the growing accessibility of biotechnology. In the long term, unexpected or dramatic shifts in key areas, including biotechnology, global biosurveillance capability and response capacity, and disease prevention and treatment, may cause the risk to change. As such, these key areas present important opportunities
for managing biological risk into the future, risk that must be addressed in a sustainable way.

The Department performed an in-depth examination of the risk associated with biological threats and hazards in the homeland security mission space. From this analysis, we identified four biological threats and hazards—referred to here as “priority biological threats and hazards”—that pose particularly high risk to the Nation and that an effective homeland security strategy for managing biological risk must address:

- Pathogens posing particular bioterrorism concerns (e.g., anthrax, plague, and smallpox), including enhanced and advanced pathogens;
- Emerging infectious diseases that are highly disruptive (e.g., viruses that could cause human pandemic);
- Animal diseases and plant pathogens or pests that are highly disruptive (e.g., foot-and-mouth disease); and
- Bioterrorist contamination of the food supply chain and water systems.

Incidents involving these priority biological threats and hazards are often difficult to prevent and can cause severe consequences, including mass illnesses, fatalities, and widespread

Table 3: The following table shows how priority areas of emphasis for the homeland security strategy for countering biological threats and hazards map to the homeland security missions.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent Biological Incidents from Occurring, When Possible</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Improve Risk Informed Decision Making</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Identify Biological Incidents Early</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Improve Confidence to Act</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Respond and Recover from Biological Incidents</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Maintain Vital Services and Functions During and After Biological Incidents</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
disruption of our society and economy. These types of threats and hazards may evade early detection; may spread quickly across regions, countries, and continents; and may persist for long periods of time. An incident involving a priority biological threat or hazard is referred to here as a “priority biological incident.”

A HOMELAND SECURITY STRATEGY FOR MANAGING BIOLOGICAL RISK

Numerous departments and agencies at the federal, state, local, tribal, and territorial levels, as well as the private sector, contribute to the national effort to address these biological threats and hazards. The Department of Health and Human Services (HHS) is the principal federal agency for protecting the Nation’s health and providing essential human services. HHS leads the Nation in preparing for, responding to, and recovering from the adverse health effects of public health incidents and develops the National Health Security Strategy. The Departments of Agriculture, Defense, Justice, the Environmental Protection Agency, and various centers within the Office of the Director of National Intelligence also perform central roles. The FBI leads investigations when an act of bioterrorism is suspected, and is the lead law enforcement agency for investigating violations of the biological warfare and terrorism statute. This strategy focuses on those activities and responsibilities assigned to DHS through statute or presidential directive, including information sharing and analysis; threat and risk awareness; biosurveillance integration and detection; technical forensic analysis to support attribution; preparedness coordination; incident management, response, and continuity planning; critical infrastructure security and resilience coordination; and border management. While these varied responsibilities have not changed significantly, this strategy integrates and harmonizes these activities in a manner that best addresses priority biological threats and hazards.

We cannot prevent all biological incidents from occurring, nor can we simply rely on our ability to respond and recover to adequately minimize the risk of catastrophic biological incidents. Therefore, our strategy is to prevent the occurrence of priority biological incidents, where possible, but, when unable to prevent, to stop priority biological incidents from overwhelming the capacity of our state, local, tribal, and territorial partners to manage and respond. To do this, we will work to prevent the release of priority biological threat agents, either by an adversary or by accident. We will also prevent, where possible, priority biological threats and hazards from crossing the border into the United States. Understanding that we cannot prevent all biological incidents from occurring, DHS, in close collaboration with HHS, the U.S. Department of Agriculture, and DOJ, will enhance situational awareness and biosurveillance capabilities to recognize faint signals of impending or evolving priority biological incidents, so we can respond to stop escalation
and thus limit potential consequences.

We will continue to help our state, local, tribal, and territorial partners develop the capabilities necessary to manage and respond to priority biological incidents with some federal support, at levels of capacity sufficient to address a “mid-range” incident (see Figure 3). Biological incidents with a “mid-range” level of risk are those that stress state, local, tribal, and territorial capacity without overwhelming it, typically also involving federal assistance. Assuming that state, local, tribal, and territorial partners can directly manage these “mid-range” incidents with some federal assistance, DHS and our federal partners will continue to invest in and develop capabilities as appropriate to support and reinforce these state, local, tribal, and territorial capabilities. Understanding and addressing the state, local, tribal, and territorial regional variability to manage and respond to a priority biological incident will allow us to optimize capability development in accordance with

Figure 3: Priority biological incidents with a “mid-range” level of risk, accounting for both likelihood and unmitigated consequences, fall above those incidents that are effectively managed by state, local, tribal, and territorial partners as a part of day-to-day operations but below catastrophic high-risk incidents, including high-likelihood, medium-consequence incidents, and low-to-high-likelihood, high-consequence incidents. The levels of likelihood and consequences that characterize a “mid-range” incident vary by priority biological threat and hazard.
STRATEGIC PRIORITIES

Presidential Policy Directive 8, “National Preparedness” (2011). This strategy is balanced and comprehensive across the different priority biological threats and hazards and across the possible actions the Department can take to reduce likelihood, mitigate vulnerabilities, and reduce consequences.

The Department will focus its resourcing efforts on capabilities necessary to prevent or stop the escalation of priority biological incidents that have the potential to reach or exceed “mid-range” risk, and on supporting response capabilities and capacities for “mid-range” priority biological incidents. What constitutes “mid-range” may vary based on the unique characteristics of different regions, jurisdictions, and localities. While implementing the strategy will result in adjustments to our long-term strategic capability and capacity development, DHS and our partners will continue day-to-day operations using current capabilities to address immediate threats and hazards. Contingency planning efforts will continue to account for all kinds of biological incidents relevant to homeland security, including low-likelihood, high-consequence biological incidents that exceed “mid-range” risk.

To execute this strategy, we will collaborate with our partners to accomplish the following six goals that involve refinements to our collective homeland security policies, capabilities, and capacities:

- Prevent or deter the release or introduction, whether intentional or inadvertent, of priority biological threats and hazards in the United States. To accomplish this goal, we will engage in activities to reduce the potential for priority biological threats and hazards to be misused or introduced into the United States, whether intentionally or inadvertently. These activities include efforts to identify, target, and interdict priority
biological threats and hazards crossing the border into the United States and supporting efforts to ensure an appropriate culture of biosafety and biosecurity in laboratory operations. While preventative in nature, these activities, along with others such as microbial forensics, also contribute to a deterrence regime that will serve to reduce the potential for deliberate or accidental release or introduction of priority biological threats and hazards.

- **Improve risk-informed decision making by ensuring decision makers at all levels across DHS and our partners are appropriately informed by a common understanding of the risk associated with priority biological threats and hazards** (e.g., potential likelihood and consequences such as illnesses/injuries, fatalities, economic impacts, and disruption to society). To accomplish this goal, DHS will work with partners to develop a common, authoritative understanding of biological risk in the homeland security mission (including potential likelihood, and consequences such as illnesses/injuries, fatalities, economic impacts, and disruption to society). DHS will also work with partners to enhance our efforts to anticipate emerging biological threats and hazards, and provide timely, accurate, and actionable information and analysis concerning these priority biological threats and hazards (at the classified/unclassified level as required).

- **Detect and confirm priority biological incidents sufficiently early to ensure incidents do not exceed state, local, tribal, and territorial capacity to manage and respond.** To accomplish this goal, DHS, in close collaboration with our partners, will refine and further integrate this detection and confirmation capability with federal, state, local, tribal, and territorial partners to achieve sufficiently accurate, timely, and trusted detection and confirmation across priority biological threats and hazards. DHS will pursue additional information sharing, integration, and analysis efforts with partners, and will reexamine information sharing policies. DHS will work with partners to pursue technological advances (e.g., information sharing and sensing/diagnostics capabilities) and translate them into deployed capabilities as they become operationally feasible and affordable.

- **Improve the confidence of our partners to act by ensuring that decision makers at all levels of government have timely, relevant, accurate, and trusted information that supports decision making.** Trusted information that gives decision makers confidence to act includes threat indications and warnings, detection tools, impact assessments, attack or disease emergence notifications, test sensitivity/specificity, and other elements. Early notification maximizes the time available for decision
makers to effectively respond. Accurately confirming and characterizing an incident and rapidly disseminating appropriate information to decision makers at all levels maximizes decision making confidence. Tabletop exercises help decision makers understand how to use information and make rapid decisions during a crisis.

- **Enable effective response to and recovery from priority biological incidents.** DHS and our partners should aim to have the collective capabilities and capacities to address what might be expected from a “mid-range” priority biological incident (see Figure 3) that would exceed the time phase, geographic scope, and casualty levels of most other threats and hazards. To accomplish this goal, we will work to ensure state, local, tribal, and territorial governments and critical infrastructure owners and operators achieve sufficient capabilities and capacities to provide lifesaving medical support and services; stabilize food, agriculture, and other critical sector functions; and minimize economic loss.

- **Maintain mission-essential functions across government and critical infrastructure services and functions during and after incidents involving priority biological threats or hazards.** To accomplish this goal, we will emphasize protection and maintenance of critical infrastructure operations that provide vital services and whose loss of functionality could negatively impact national security, economic vitality, and public health and safety in the face of a biological event. Such emphasis must form part of our risk-informed, all-hazards approach to security and resilience of critical infrastructure so that people are protected and critical facilities continue to operate. We will also encourage collaborative planning and the development and adoption of protocols and standards for protecting critical infrastructure from biological attacks. DHS will maintain our mission-essential functions and protect Department personnel against priority biological threats and hazards. DHS will provide guidance to other Federal departments and agencies and encourage our other partners to take appropriate actions to maintain mission-essential functions in the event of a priority biological incident.

**BUILDING FUTURE CAPABILITIES TO ACHIEVE SUCCESS**

The success of this strategy relies upon DHS and our partners enhancing coordination efforts and improving the confidence to act. Success also relies on increasing situational awareness by further integrating and coordinating the collection, analysis, and sharing of information, as appropriate, to proactively address priority biological threats and hazards. Before making any substantial new investments, DHS will thoughtfully examine the way our current efforts are being executed in order to identify untapped efficiencies.
A RISK SEGMENTATION APPROACH TO SECURING AND MANAGING FLOWS OF PEOPLE AND GOODS

OVERVIEW

DHS and our partners secure and manage the flows of people and goods to enable prosperity and minimize risk. We ensure transit via legal pathways; identify and remove people and goods attempting to travel illegally; and ensure the safety and integrity of these flows of people and goods by safeguarding the conveyances, nodes, and pathways that make up the travel and trade system. This includes our responsibilities in border security, trade law compliance, transportation security, and immigration, among others.

Expediting and safeguarding trade and travel while deterring and interdicting illicit traffic requires understanding how flows of people and goods interact with each other and with external forces. For example, transnational criminal organizations are highly dynamic, and will often respond to pressure on one illicit flow by shifting to another product or route. Similarly, as the volume of global trade and travel increases, the potential for harmful diseases or invasive species to cross our borders also increases.
Table 4: The following table shows how priority areas of emphasis for a risk segmentation approach to securing and managing flows of people and goods map to the homeland security missions.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimize Disruption to and Facilitate Safe and Secure Inbound and Outbound Legal Flows of People and Goods</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Prioritize Efforts to Counter Illicit Finance and Further Increase Transnational Criminal Organization Perception of Risk, While Continuing to Increase Efficiencies in Operations</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Prevent Terrorist Travel into the United States, Terrorism Against International Travel and Trade Systems, and the Export of Sensitive Goods and Technology</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

SEGMENTING FLOWS OF PEOPLE AND GOODS

We identified three distinct but interrelated types of flows of people and goods based on an in-depth look at legal and illegal flows. Each type requires a different approach by DHS and our partners:

- **Legal Flows of People and Goods.** The vast majority of people and goods entering and exiting the United States represents lawful travel and trade. DHS and our partners work to secure and expedite these flows of people and goods, as they are a main driver of U.S. economic prosperity.

- **Market-Driven Illicit Flows of People and Goods.** These flows of people and goods are characterized by the exploitation of legitimate trade, travel, and financial systems or the creation of alternative, illicit pathways through which people and illegal goods—narcotics, funds, counterfeits, and weaponry—can cross the border. Primarily driven by criminal profits, these flows of people and goods are persistent and enduring. The risk from these activities is difficult to mitigate, especially given the limited role of homeland security activity in addressing the root causes of supply and demand.
• **Terrorism and Other Non-Market Concerns.** These flows of people and goods are driven by social, political, natural, or other non-market forces. These flows of people and goods are illegal, attempt to hide within legal flows or illicit flows that bypass ports of entry, and have the potential to overwhelm the legal trade and travel system or threaten national security. Examples include terrorists; migration driven by displacement or political fears; and the movement of diseases, pests, and invasive species.

Segmenting flows of people and goods in this way permits more focused strategies and more efficient allocation of resources.

**A HOMELAND SECURITY APPROACH TO FLOWS OF PEOPLE AND GOODS**

Our approach to flows of people and goods focuses on achieving three strategic objectives: (1) minimize disruption to and facilitate safe and secure inbound and outbound legal flows of people and goods; (2) prioritize efforts to counter illicit finance and further increase transnational criminal organizations’ perception of risk through targeted interdiction and other activities, while continuing to increase efficiencies in operations; and (3) prevent terrorist travel into the United States, terrorism against international travel and trade systems, and the export of sensitive goods and technologies.

**MINIMIZE DISRUPTION TO AND FACILITATE SAFE AND SECURE INBOUND AND OUTBOUND LEGAL FLOWS OF PEOPLE AND GOODS**

Challenges to flows of people and goods are not limited to illegal activity. Trends indicate higher volumes of trade and travel could overwhelm our port of entry infrastructure and
strain frontline personnel. Aging infrastructure needs to be upgraded at air, land, and sea ports of entry.

We must also manage those threats and hazards that pose risk to the trade and travel system. We do this by sorting traveler and cargo traffic based on risk and expediting the movement of those found to be low risk. We partner with airlines, cargo carriers, and other relevant organizations to expedite legal flows of people and goods without compromising security. Pre-inspection capabilities, advanced analytics, and mutual recognition agreements with our international partners will further increase the use of traffic segmentation programs. Sorting traffic by risk also helps address terrorism threats, as discussed in the Securing Against the Evolving Terrorism Threat subsection.

Partnerships that leverage the overlapping interests, resources, and authorities of our partners in both the public and private sectors are essential to meet mutual safety and security needs while expediting trade and travel. Public-private partnerships are an important but underutilized resource, and we describe how to improve them in the Strengthening the Execution of Our Missions through Public-Private Partnerships subsection.

PRIORITIZE EFFORTS TO COUNTER ILLICIT FINANCE AND FURTHER INCREASE TRANSONATIONAL CRIMINAL ORGANIZATION PERCEPTION OF RISK THROUGH TARGETED INTERDICTI0N AND OTHER ACTIVITIES, WHILE CONTINUING TO INCREASE EFFICIENCIES IN OPERATIONS

Our analysis identified two areas where DHS intervention can have an especially high impact: (1) targeting the profits of market-driven criminal activity and (2) increasing the perception of risk transnational criminal organizations face in attempting to serve U.S. markets. Our operations directed at market-driven illicit activities also need to become more efficient.
Targeting the profits of market-driven criminal activity eliminates the motive to conduct that activity. Illicit finance is the common factor across all illicit market-driven flows of people and goods. Our efforts should target illicit financing activities that transnational criminal organizations depend on, such as money laundering, and increase outbound inspection to deter practices such as cash smuggling or the use of stored-value media.

Transnational criminal organizations remain the primary adversary in market-driven flows of people and goods, and maximizing profit continues to be their major incentive. Although directly targeting the illegal movement of people and goods has resulted in reductions to specific flows, transnational criminal organizations are highly dynamic and will often respond to pressure on one illicit flow by shifting to another product or route. For that reason, it is difficult to assess the long-term effectiveness of specific actions on transnational criminal organization decision making. Homeland security activities must therefore create a deterrent effect, injecting the greatest amount of uncertainty and concern into that decision making. Examples of these types of activities include swiftly shifting assets, presence, technology, and tools, further targeting and focusing interdiction activities, and emphasizing strategic communications that project the effectiveness of homeland security capabilities.

We must also increase efficiencies in how we acquire, govern, and employ our capabilities for managing market-driven illicit activities. This includes (1) integrating capital acquisition and major investments across government; (2) increasing joint governance structures and collaboration to leverage assets, such as the National Targeting Center; and (3) shifting activities that have a lower impact on the overall system to lower-cost solutions.

**Prevent Terrorist Travel into the United States, Terrorism Against International Travel and Trade Systems, and the Export of Sensitive Goods and Technology**

Countering terrorism within the travel and trade system is a priority because (1) we must prevent violent extremists from exploiting legal and illegal pathways to enter the United States, and (2) attacks against the trade and travel system can cause major system disruption to American life and global commerce.

We must work with our partners in the Departments of Justice, Commerce, Energy, and elsewhere to prevent the export, re-export, or transfer of certain advanced technology and sensitive goods and technologies (e.g., restricted military and dual-use items) that could threaten the security of the United States and our allies if they fell into the wrong hands. Countering terrorism is further discussed in the Securing Against the Evolving Terrorism Threat subsection.
STRENGTHENING THE EXECUTION OF OUR MISSIONS THROUGH PUBLIC-PRIVATE PARTNERSHIPS

OVERVIEW

Homeland security is achieved through a shared effort among all partners, from corporations to nonprofits and American families. Together, we can harness common interests to achieve solutions beyond what any of us could do alone. The first Quadrennial Homeland Security Review highlighted the need to mature and strengthen international partnerships as well as partnerships with state, local, tribal, and territorial governments. Building on that foundation, the second quadrennial review focuses on enhancing the critical relationship between government and the private sector.

Partnerships have always been fundamental to homeland security. Public-private partnerships advance the security and resilience of critical infrastructure under the National Infrastructure Protection Plan. Government relationships and agreements with airlines, shippers, and multi-national corporations facilitate the lawful flows of people and goods while enhancing security and screening capabilities. The Whole Community initiative for national preparedness and resilience supports the creation of critical preparedness
partnerships long before disasters occur. The Captain of the Port relationship, which combines a mix of authorities, regulatory regimes, and proactive collaboration among state and local agencies, industry, and port partners, strikes an important balance between regulation and partnership. This relationship encourages the use and creation of reasonable and fair regulations and fosters industry-led innovations in maritime safety and response technologies. The Air Cargo Advance Screening pilot program was built from the ground up in coordination with industry in response to al-Qa‘ida in the Arabian Peninsula’s 2010 attempt to attack the international air cargo system by detonating explosive devices hidden in air cargo shipments from Yemen to the United States. The Air Cargo Advance Screening pilot program is widely considered one of the best examples of homeland security partnership within both the public and private sectors.

Still, the Department can go further to advance a consistent, structured approach to partnerships as well as to enhance institutional awareness of public-private partnerships. The following framework outlines that structured approach and can be found in more detail in the Partnerships Toolkit, available at http://www.dhs.gov/qhsr.

Table 5: The following table shows how priority areas of emphasis for strengthening the execution of our missions through public-private partnerships map to the homeland security missions.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Institutionalize a structured approach to developing public private partnerships, to include homeland security partnership archetypes linked to specific desired outcomes</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Establish a homeland security Community of Practice to identify potential partnership opportunities, develop a repository of partnerships and best practices, and serve as a consultative body to inform the exploration and formation of new partnerships</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
A STRUCTURED APPROACH TO PUBLIC-PRIVATE SECURITY AND RESILIENCE PARTNERSHIPS

ALIGNED INTERESTS AND SHARED OUTCOMES

At a time when we must do more with less, two guiding principles help public-private partnerships maximize the investment by each partner and the success of the partnership: (1) aligning interests and (2) identifying shared outcomes.

By focusing on how interests align, we can provide alternatives to costly incentives or regulations and help ensure a partnership is based on a solid foundation of mutual interest and benefit. There are many examples of public and private sector interests aligning in homeland security. Common interests include the safety and security of people and property, the protection of sensitive information, effective risk management, the development of new technology, reputation enhancement, and improved business processes. New ways of thinking about corporate social responsibility—in which societal issues are held to be core business interests rather than traditional philanthropy—also present an opportunity to identify shared interests.

Where interests do not directly align, potential partners can often be motivated by shared desired outcomes, such as enhanced resilience; effective disaster response and recovery; and greater certainty in emerging domains, such as cyberspace and the Arctic.

Despite the existence of shared interests and mutual desired outcomes, challenges will exist. Partnerships must often overcome inherent differences in motivations and operational cultures, including risk tolerance, funding, and time horizons. The government must also be mindful to avoid suggesting a preferred relationship, endorsing a partner, or the appearance of privileged access or unfair competition. Being aware of, respecting, and creatively addressing these differences create an essential foundation for public-private partnerships.

PARTNERSHIP ARCHETYPES FOR HOMELAND SECURITY

Successful, well-organized partnership frameworks begin with a set of flexible models for current and future partnerships. For decades, industries, such as construction and international development, have employed public-private partnership models to bring organization and definition to partnerships and provide a basic starting point for developing future partnerships. Flexible models also provide a foundation for thinking about partnership objectives, potential partners, and the resources and capabilities needed to address varying challenges.
Within homeland security, there are five partnership archetypes that encompass the types of relationships we share with the private sector, as shown in Table 6. These archetypes are tied to unique desired outcomes and are arrayed across a spectrum according to depth, investment, and complexity. For well-known challenges, where roles and responsibilities are clearly documented, partnership models can be applied directly. As problems increase in complexity and risk, however, the flexible models can be adapted, scaled, or even combined to achieve desired outcomes.

**THE PATH FORWARD: A PARTNERSHIP CULTURE FOR HOMELAND SECURITY**

Building on the foundation of the archetypes, we can begin to apply common lessons learned and best practices, spark new and innovative partnerships, and develop crucial relationships long before crises occur. We will build a Department-wide Community of Practice to synchronize the identification of potential partnership opportunities, develop a repository of partnerships and best practices, and serve as a consultative body to inform the exploration and formation of new partnerships, in close collaboration with other federal agencies and the private sector. In addition, we must highlight the importance of partnerships in training and education activities to build the skills needed to identify and negotiate successful partnerships. By developing this shared expertise, we will create, enhance, and sustain our essential relationship with the private sector.
6. AREAS OF ONGOING PRIORITY AND EMPHASIS

While the Strategic Priorities section of this report describes strategic shifts and new areas of priority, this section reflects certain key ongoing priorities and areas of emphasis for homeland security, driven by risk and long-standing policy imperatives.

NUCLEAR TERRORISM USING AN IMPROVISED NUCLEAR DEVICE

OVERVIEW

Nuclear terrorism remains an enduring risk because of its potential consequences, and as such, preventing nuclear terrorism is a national security priority for the United States. As President Obama stated in his speech at South Korea’s Hankuk University in March 2012, “We know that just the smallest amount of plutonium—about the size of an apple—could kill hundreds of thousands and spark a global crisis. The danger of nuclear terrorism remains one of the greatest threats to global security.” A terrorist nuclear attack on the Nation would cause severe loss of life, illness, and injury; present challenges to our economy and our free and open society; and damage the national psyche. While the difficulty of stealing
a nuclear weapon or fabricating one from stolen or diverted weapons materials reduces the likelihood of this type of attack, the extremely high consequences of an improvised nuclear device attack make it an ongoing top homeland security risk.

**STRATEGIC APPROACH**

We prioritize a sustained, long-term focus on preventing nuclear terrorism through two foundational capabilities: (1) nuclear detection and (2) nuclear forensics. These capabilities are aimed at preventing our adversaries from developing, possessing, importing, storing, transporting, or using nuclear materials. While we have made significant progress in both detection and forensics over the years, the threat of nuclear terrorism is persistent and requires constant vigilance.

DHS and other departments and agencies have combined their authorities and assets to build the U.S. Government’s global nuclear detection capability through the Global Nuclear Detection Architecture, a world-wide network of sensors, people, and information designed to encounter, detect, characterize, and report on nuclear material out of regulatory control. Not only does the Global Nuclear Detection Architecture help reduce the likelihood that radiological or nuclear material can be used as a weapon against the Nation, but by
increasing the cost, difficulty, and risk of attempting a nuclear attack, it also acts to deter those who may seek to attack us. The Global Nuclear Detection Architecture presents terrorists with many obstacles to a successful attack, greatly increasing their cost, difficulty, and risk, and thereby deterring terrorists. Through this detection architecture, departments and agencies train personnel, deploy detection systems at home and abroad, and analyze the data these systems generate. Federal, state, local, tribal, territorial, and international partners, as well as many others, are engaged in this effort.

While Global Nuclear Detection Architecture capabilities are focused primarily against terrorists, federal department and agency nuclear forensics capabilities target the decision making of would-be state sponsors. Terrorists can only acquire the special nuclear material necessary for a nuclear weapon by theft, illicit trafficking, or direct support from a state. Thus, nuclear forensics efforts are focused on deterring potential state sponsors of nuclear terrorism by denying them anonymity and ensuring they be held accountable.

As stated in the Nuclear Posture Review (2010), the United States is committed to hold fully accountable any state, terrorist group, or other non-state actor that supports or enables terrorist efforts to obtain or use weapons of mass destruction. Our commitment is made possible by our ability to identify perpetrators through information gained from nuclear forensics, intelligence, and law enforcement. Such information serves as a strong deterrent to terrorist accomplices and especially to potential state sponsors of terrorism. Federal agencies work with our National Technical Nuclear Forensics Center to ensure the Nation’s nuclear forensics capability is continually advancing and is ready to respond to a nuclear trafficking incident or a terrorist nuclear attack.

We can leverage these nuclear detection and forensics capabilities to influence the decision making of key actors in a potential terrorist nuclear attack or radiological attack, thereby reducing its likelihood.

We complement our operational efforts with extensive analysis aimed at understanding radiological and nuclear terrorism risk. This analysis has matured to a point where we can understand and discern different levels of risk posed by the various pathways and mechanisms for introducing an improvised nuclear device into the United States, not simply the potential consequences of such an introduction. Consequently, we balance our efforts across pathways commensurate with the risk that each one poses.
IMMIGRATION

OVERVIEW

Immigration is essential to our identity as a nation of immigrants. Most American families have an immigration story, some recent, some more distant. Many immigrants have taken on great risks to come to our country and seek to work and contribute to America’s prosperity or were provided refuge after facing persecution abroad. Americans are extremely proud of this tradition.

Immigration will always be, first and foremost, an opportunity for our country. We reap great economic benefits from receiving the best, brightest, and most hardworking people from across the globe. Immigrants also build bridges to other nations, personally extending our diplomatic reach. They serve in our military and intelligence services with honor, sometimes contributing important language and cultural skills. Immigration enhances how the United States is perceived—as a cosmopolitan nation made up of many cultures and as a champion of humanitarian causes around the world.
Smart and effective enforcement and administration of our immigration laws remains a core homeland security mission. But even though we have already made significant improvements to border security, interior enforcement, and benefits adjudication, our current immigration system remains broken, and it remains an economic, humanitarian, and national security imperative to fix it. Our country needs an immigration system that better supports family reunification, meets the demands of our growing economy, extends humanitarian protections to those in need, and gives undocumented immigrants a path to earned citizenship. Enactment of comprehensive immigration reform thus remains a top homeland security priority.

The President has established four core objectives for strengthening our immigration system through common-sense immigration reform:

- Continuing to strengthen border security;
- Cracking down on employers that hire undocumented workers;
- Creating a path to earned citizenship; and
- Modernizing and streamlining our legal immigration system.

To accomplish these objectives, homeland security partners and stakeholders must function as an interconnected whole. DHS and the Departments of State, Justice, Education, Health and Human Services, and Labor all work to facilitate lawful immigration and to identify and remove threats to our national security and public safety. Further, state and local governments and law enforcement, businesses large and small, and nongovernmental and voluntary organizations also play important roles in our immigration system. For example, government and voluntary organizations together support new refugee arrivals, and government and employers cooperate to ensure that employees are working legally and to prevent employers from discriminating against employees when verifying their authorization to work in the United States. The Federal Government and state and local law enforcement agencies coordinate as appropriate to identify those who pose a national security or public safety risk, so the Federal Government can pursue appropriate enforcement action.

As the President stated in his 2014 State of the Union address, Congress must enact common-sense, comprehensive immigration reform.
STRATEGIC SHIFTS IN IMMIGRATION

BUILDING A STRONGER, SMARTER BORDER ENFORCEMENT SYSTEM

Our immigration system continues to prioritize the security of our border and its arrival zones. As with other flows of people and goods (described in the A Risk Segmentation Approach to Securing and Managing Flows of People and Goods subsection), we take a risk-informed, intelligence-driven, and networked approach to enforcing immigration laws. We have built a border security system that is stronger than ever before; the Border Patrol has doubled from approximately 10,000 agents in 2004 to 21,370 in 2014. Investigative resources have also expanded. The Federal Government works closely with state, local, tribal, and territorial partners to identify concerns at our borders, whether they occur on land, via air routes, or at sea.

Securing the border is not just about adding more resources; it is about using the resources we have in a smarter way. We have deployed a vast array of new technologies at and between points of entry. For example, unmanned aerial surveillance tools now can cover the southwest border from California to Texas. More traditional border security tools also remain available to enhance border security. We continue to deploy fixed and mobile surveillance capabilities on the ground, allowing more agents to shift from detection duties to increase our capacity to respond, interdict, and resolve illegal activities. We will continue to operate in a manner that protects privacy and civil liberties and respects humanitarian interests.

The security of the U.S. immigration system can only be ensured by cooperating with foreign states. Through the U.S.-Canada Beyond the Border initiative and the U.S.-Mexico Declaration on 21st-Century Border Management, we are working to harmonize processing inspection and data-sharing efforts with the Governments of Mexico and Canada. We have also concluded agreements with Caribbean countries lending support to U.S. Coast Guard rescue and interdiction operations at sea. In Central America, in collaboration with our
partners, we are focusing public messaging and diplomatic engagement efforts, in conjunction with the Department of State, on countries that have been increasing sources of illegal migration. In other countries, U.S. visa security program officers continue to prevent travel by those who pose a threat. We will continue to secure the border by cooperating with foreign allies.

Together, these efforts are making concrete improvements in our homeland security. We will continue to build on this progress, enhancing infrastructure and deploying technology to strengthen our ability to keep out criminals and national security threats. Comprehensive immigration reform, including enhanced penalties against criminals, would facilitate this effort.

ACHIEVING SMART AND EFFECTIVE INTERIOR ENFORCEMENT

DHS and our partners are taking a more effective approach to interior enforcement. In particular, we prioritize removing those posing threats to national security, border security, or public safety—aliens engaged in or suspected of terrorism or espionage and aliens convicted of crimes—while protecting victims of crime and human trafficking. We also prioritize prosecuting priority cases, such as against unscrupulous employers and transnational criminal organizations involved in document fraud, trafficking, and human smuggling, while using prosecutorial discretion on a case-by-case basis and as appropriate.

Our worksite enforcement strategy uses other tools, such as audits and civil fines, to penalize employers who knowingly hire illegal workers. We also promote compliance through E-Verify, a web-based service that allows employers to verify whether their employees are eligible to work in the United States. Approximately 520,000 employers representing more than 1.4 million worksites are enrolled in the E-Verify program, including employers with federal contract positions.

While we use many means to effectively secure the Nation’s interior, these efforts can only go so far. Comprehensive immigration reform is needed to enable businesses to employ a legal workforce through programs, such as mandatory employment verification, and more stringent penalties for those who violate the law.
CREATING A 21ST-CENTURY LEGAL IMMIGRATION SYSTEM

We are also committed to creating an immigration system that better meets our diverse economic needs. Such a system requires comprehensive immigration reform. Existing numerical limits within our immigration system ignore the needs of today’s economy and constrain the benefits immigrants bring to our country. Further, workers need better mobility and additional protections to reduce the risk that they will be exploited. Comprehensive immigration reform is needed to reorient our immigration system to meet the needs of the marketplace.

In the meantime, we are working to better assist high-skilled immigrants. Entrepreneurs and government officials leveraged knowledge from our best and brightest through the Entrepreneurs-in-Residence initiative, streamlining DHS policies and practices to better reflect the realities faced by foreign entrepreneurs and start-up businesses. We have continued to use industry-specific Executives in Residence to ensure consistency in adjudications within the performing arts, entertainment, and nursing industries. We are also streamlining the processing of immigrant visas to encourage businesses to grow in the United States. For students, the Study in the States program provides concrete immigration guidance to those who want to study here. We will continue to develop innovative programs to enable immigrants to reach their potential in the United States.

ADDRESSING LENGTHY VISA BACKLOGS

Perhaps nowhere is there greater evidence of a broken immigration system than in the burdensome backlogs for family-based immigrants waiting for visa numbers to become available. Many family members face a wait time of a decade or more just for the chance to reunite with family members in the United States. While we already work to identify solutions on a case-by-case basis, more can and should be done.

Comprehensive reform of our family-based immigration system is needed to reunite families in a timely manner consistent with our values. One important reform would change numerical limits on family-sponsored immigration, significantly reducing the years of separation these families now endure.

EARNED PATH TO CITIZENSHIP

Today, we have an estimated 11.5 million immigrants living in America without documentation. The overwhelming majority does not pose a threat; these individuals seek only to be fully contributing members of their communities. We support comprehensive immigration reform that would provide an earned pathway to citizenship for these persons. Qualified applicants would be required to register and undergo national security and
AREAS OF ONGOING PRIORITY AND EMPHASIS

criminal background checks, pay taxes and a fine, and fully integrate into the United States by learning English.

Our country is stronger and more secure when everyone has a stake, fulfills his or her responsibilities, and is equally invested in our common future. Comprehensive immigration reform would represent a unique opportunity to improve homeland security.

ENHANCING MANAGEMENT AND ORGANIZATION TO DEVELOP A RESPONSIVE IMMIGRATION SYSTEM

At the center of any good immigration system must be an administrative structure able to rapidly respond to changes in demand while safeguarding security. We are constantly seeking ways to better administer benefits, clarify what is required of applicants, and use technology to make information more accessible. Based on feedback from our partners, DHS has implemented programs to support naturalization applicants and to help the public as the Department transforms from paper-based to electronic processing.

It is well understood that comprehensive immigration legislation will significantly increase pressures on our administrative system. We will work hard to ensure we have the capacity, staff, and resources to successfully implement any changes in the law. Following DHS’s decision in June 2012 to extend consideration of deferred action for childhood arrivals—a process to allow undocumented young people who meet certain guidelines to remain and work in the United States—the Department received and processed more than a half-million deferred action requests in less than a year. We can and will build upon these successes.
NATIONAL PREPAREDNESS AND THE WHOLE COMMUNITY APPROACH

OVERVIEW

National preparedness is a top Administration priority and an enduring homeland security focus. Indeed, national preparedness underpins all efforts to safeguard and secure the Nation against those threats and hazards that pose the greatest risk. Given the evolving terrorism threat; the growing risk of cyber disruptions; enduring hazards, such as biological challenges and nuclear terrorism; and the increasing number of natural disasters with more costly and variable consequences—driven by trends, such as climate change, aging infrastructure, and shifts in population density to higher-risk areas—it is imperative to build and sustain core capabilities to prevent, protect against, mitigate, respond to, and recover from the most high-risk threats and hazards. Continued integration and increased coordination provide a mechanism for achieving greater national preparedness among homeland security partners within resource limits.
STRATEGIC APPROACH

Presidential Policy Directive 8 calls for a National Preparedness Goal (the Goal) that identifies the core capabilities necessary to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk; a National Preparedness System composed of guidance, programs, and processes to guide activities to achieve the Goal; and a comprehensive Campaign to Build and Sustain Preparedness to unify efforts across the Whole Community to build and sustain national preparedness. Presidential Policy Directive 8 reinforces and complements the authorities set forth in the Post-Katrina Emergency Management Reform Act of 2006. These key national preparedness elements include the following:

- **The National Preparedness Goal:** The Goal defines what it means for the Nation to be prepared for the threats and hazards that pose the greatest risk, including acts of terrorism, cyberattacks, pandemics, and catastrophic natural disasters. The Goal is “[a] secure and resilient Nation with the capabilities required across the Whole Community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.”

- **The National Preparedness System:** The National Preparedness System provides a consistent approach that supports decision making, resource allocation, and the measurement of progress toward achieving the Goal. The National Preparedness System includes but is not limited to the following:

  - **National Planning Frameworks and the Federal Interagency Operational Plans:** The Federal Emergency Management Agency (FEMA) and its partners completed first editions of the National Prevention Framework, National Protection Framework, National Mitigation Framework, and National Disaster Recovery Framework, as well as the second edition of the National Response Framework. Together, these National Planning Frameworks describe how the Whole Community works together to prevent, protect against, mitigate, respond to, and recover from threats and hazards. Each framework is supported by a Federal Interagency Operational Plan, which explains how federal departments and agencies work together to deliver the core capabilities through the coordinating mechanisms outlined in the framework. The Protection Federal Interagency Operational Plan is under development. The frameworks are built upon scalable, flexible, and adaptable coordinating
structures that align key roles and responsibilities to deliver necessary capabilities.

- **Catastrophic Planning:** Catastrophic planning is performed both at FEMA Headquarters and the FEMA regional offices in collaboration with the Whole Community and includes planning for National Special Security Events.

- **National Exercise Program:** The National Exercise Program serves as the cornerstone of a collective effort to test, improve, and assess national preparedness. The program seeks to enhance resilience at all levels of government, within nonprofit, faith-based, and nongovernmental organizations and throughout the private sector. It employs a finite series of progressive exercises that test the ability to prevent, protect against, mitigate, respond to, and recover from all hazards.

- **National Preparedness Report:** The annual National Preparedness Report summarizes national progress in building, sustaining, and delivering the 31 core capabilities outlined in the Goal, based on analysis from ongoing national preparedness assessments.

- **Campaign to Build and Sustain Preparedness:** The Campaign has four key elements: (1) a comprehensive campaign, including public outreach and community-based and private sector programs; (2) federal preparedness efforts; (3) grants, technical assistance, and other federal preparedness support; and (4) research and development. This initiative provides a structure for integrating new and existing community-based, nonprofit, and private sector preparedness programs, research and development activities, and preparedness assistance. Further, the Campaign is designed to provide consistent and constant outreach to the public to help ensure the basic tenets of the Goal are understood and met.

Recognizing that preparedness is a shared responsibility, the Whole Community approach calls for the involvement of everyone—not just the government—in preparedness efforts. By working together, everyone can keep the Nation safe from harm and resilient when struck by hazards. The Whole Community approach is based on three core principles: (1) understanding and meeting the actual needs of the Whole Community; (2) engaging and empowering all parts of the community; and (3) strengthening what works well in communities on a daily basis. Whole Community is a means by which residents, emergency managers, organizational and community leaders, government officials, private and nonprofit sectors, faith-based and disability organizations, and the general public can
collectively understand and assess the needs of their respective communities as well as determine the best ways to organize and strengthen their assets, capacities, and interests. A Whole Community approach to planning and implementing disaster strategies helps build a more effective path to societal security and resilience.

Whole Community includes the following:

- Individuals and families, including those with access and functional needs;
- Businesses;
- Faith-based and community organizations;
- Nonprofit groups;
- Schools and academia;
- Media outlets; and
- All levels of government, including federal, state, local, tribal, and territorial partners.

The Whole Community approach helps each community make smart decisions about how to manage those segments of the community. This includes accounting for the composition of the community, the individual needs of community members of every age and income level, and all accessibility requirements. It also helps residents, emergency managers, organizational and community leaders, government officials, private and nonprofit sectors, faith-based and disability organizations, and the general public to collectively understand community needs and how to organize resources to meet those needs. Supporting this process, state, local, tribal, and territorial governments identify their risks and make decisions for addressing their greatest risks through the completion of the Threat and Hazard Identification and Risk Assessment process.

In this manner, national preparedness increases security and resilience by helping our Nation systematically prepare for the threats and hazards that pose the greatest risk.
7. MISSION FRAMEWORK IN DEPTH

The first quadrennial review developed an enduring framework of missions and associated goals that tell us in detail what it means to ensure a safe, secure, and resilient Nation, as well as how to go about the business of conducting homeland security. These missions are not limited to DHS—hundreds of thousands of people from across the Federal Government; state, local, tribal, and territorial governments; the private sector; and other nongovernmental organizations are responsible for executing these missions. These homeland security professionals are responsible for public safety and security. They regularly interact with the public; facilitate and expedite legal trade and travel; own and operate our Nation’s critical infrastructure and services; perform research and develop technology; and keep watch for, prepare for, deter, anticipate, and respond to emerging threats and hazards. As our partners carry out their homeland security responsibilities, the homeland security mission framework serves as a guidepost and provides clarity and unity of purpose.
The updated missions and goals set forth in this second Quadrennial Homeland Security Review report reflect changes in the strategic environment and areas where homeland security partners and stakeholders have matured, evolved, and enhanced their capabilities and understanding of the homeland security mission space:

**MISSION 1: PREVENT TERRORISM AND ENHANCE SECURITY**

**Goal 1.1: Prevent Terrorist Attacks**
- Analyze, fuse, and disseminate terrorism information;
- Deter and disrupt operations;
- Strengthen transportation security; and
- Counter violent extremism.

**Goal 1.2: Prevent and Protect Against the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities**
- Anticipate chemical, biological, radiological, and nuclear emerging threats;
- Identify and interdict unlawful acquisition and movement of chemical, biological, radiological, and nuclear precursors and materials; and
- Detect, locate, and prevent the hostile use of chemical, biological, radiological, and nuclear materials and weapons.

**Goal 1.3: Reduce Risk to the Nation’s Critical Infrastructure, Key Leadership, and Events**
- Enhance security for the Nation’s critical infrastructure from terrorism and criminal activity; and
- Protect key leaders, facilities, and national special security events.
MISSION 2: SECURE AND MANAGE OUR BORDERS

Goal 2.1: Secure U.S. Air, Land, and Sea Borders and Approaches
- Prevent illegal import and entry; and
- Prevent illegal export and exit.

Goal 2.2: Safeguard and Expedite Lawful Trade and Travel
- Safeguard key nodes, conveyances, and pathways;
- Manage the risk of people and goods in transit; and
- Maximize compliance with U.S. trade laws and promote U.S. economic security and competitiveness.

Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations and Other Illicit Actors
- Identify, investigate, disrupt, and dismantle transnational criminal organizations; and
- Disrupt illicit actors, activities, and pathways.

MISSION 3: ENFORCE AND ADMINISTER OUR IMMIGRATION LAWS

Goal 3.1: Strengthen and Effectively Administer the Immigration System
- Promote lawful immigration;
- Effectively administer the immigration services system; and
- Promote the integration of lawful immigrants into American society.

Goal 3.2: Prevent Unlawful Immigration
- Prevent unlawful entry, strengthen enforcement, and reduce drivers of unlawful immigration; and
- Arrest, detain, and remove priority individuals, including public safety, national security, and border security threats.
MISSION 4: SAFEGUARD AND SECURE CYBERSPACE

Goal 4.1: Strengthen the Security and Resilience of Critical Infrastructure

- Enhance the exchange of information and intelligence on risks to critical infrastructure and develop real-time situational awareness capabilities that ensure machine and human interpretation and visualization;
- Partner with critical infrastructure owners and operators to ensure the delivery of essential services and functions;
- Identify and understand interdependencies and cascading impacts among critical infrastructure systems;
- Collaborate with agencies and the private sector to identify and develop effective cybersecurity policies and best practices; and
- Reduce vulnerabilities and promote resilient critical infrastructure design.

Goal 4.2: Secure the Federal Civilian Government Information Technology Enterprise

- Coordinate government purchasing of cyber technology to enhance cost-effectiveness;
- Equip civilian government networks with innovative cybersecurity tools and protections; and
- Ensure government-wide policies and standards are consistently and effectively implemented and measured.

Goal 4.3: Advance Law Enforcement, Incident Response, and Reporting Capabilities

- Respond to and assist in the recovery from cyber incidents; and
- Deter, disrupt, and investigate cybercrime.

Goal 4.4: Strengthen the Ecosystem

- Drive innovative and cost effective security products, services, and solutions throughout the cyber ecosystem;
- Conduct and transition research and development, enabling trustworthy cyber infrastructure;
- Develop skilled cybersecurity professionals;
- Enhance public awareness and promote cybersecurity best practices; and
- Advance international engagement to promote capacity building, international standards, and cooperation.
MISSION 5: STRENGTHEN NATIONAL PREPAREDNESS AND RESILIENCE

Goal 5.1: Enhance National Preparedness

- Empower individuals and communities to strengthen and sustain their own preparedness;
- Build and sustain core capabilities nationally to prevent, protect against, mitigate, respond to, and recover from all hazards; and
- Assist federal entities in the establishment of effective continuity programs that are regularly updated, exercised, and improved.

Goal 5.2: Mitigate Hazards and Vulnerabilities

- Promote public and private sector awareness and understanding of community-specific risks;
- Reduce vulnerability through standards, regulation, resilient design, effective mitigation, and disaster risk reduction measures; and
- Prevent incidents by establishing, and ensuring compliance with, standards and regulations.

Goal 5.3: Ensure Effective Emergency Response

- Provide timely and accurate information;
- Conduct effective, unified incident response operations;
- Provide timely and appropriate disaster assistance; and
- Ensure effective emergency communications.

Goal 5.4: Enable Rapid Recovery

- Ensure continuity and restoration of essential services and functions; and
- Support and enable communities to rebuild stronger, smarter, and safer.
MATURE AND STRENGTHEN HOMELAND SECURITY

The strategic aims and objectives for Maturing and Strengthening Homeland Security are drawn from the common themes that emerge from each of the homeland security mission areas.

Integrate Intelligence, Information Sharing, and Operations

- Enhance unity of regional operations coordination and planning;
- Share homeland security information and analysis, threats, and risks;
- Integrate counterintelligence;
- Establish a common security mindset; and
- Preserve civil liberties, privacy, oversight, and transparency in the execution of homeland security activities.

Enhance Partnerships and Outreach

- Promote regional response capacity and civil support;
- Strengthen the ability of federal agencies to support homeland security missions;
- Expand and extend governmental, nongovernmental, domestic, and international partnerships; and
- Further enhance the military-homeland security relationship.

Conduct Homeland Security Research and Development

- Scientifically study threats and vulnerabilities;
- Develop innovative approaches and effective solutions; and
- Leverage the depth of capacity in national labs, universities, and research centers.

Train and Exercise Frontline Operators and First Responders

- Enhance systems for training, exercising, and evaluating capabilities; and
- Support law enforcement, first responder, and risk management training.

Strengthen Service Delivery and Manage DHS Resources

- Recruit, hire, retain, and develop a highly qualified, diverse, effective, mission-focused, and resilient workforce; and
- Manage the integrated investment life cycle to ensure that strategic and analytically-based decisions optimize mission performance.
8. CONCLUSION

Four years ago, the first quadrennial review defined homeland security for America in the 21st century as a concerted national effort to ensure a Nation that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive.

Since then, we have developed capabilities and processes to become more risk based, more integrated, and more efficient. This second quadrennial review describes how those capabilities and processes inform us of what challenges lie ahead and how to strategically posture ourselves to address those challenges.

Based on the strategic environment, the drivers of the most significant risk, and our guiding principles, the second Quadrennial Homeland Security Review identifies the following strategic priorities, which cut across the five homeland security missions:
CONCLUSION

- An updated posture to address the increasingly decentralized terrorist threat;
- A strengthened path forward for cybersecurity that acknowledges the increasing interdependencies among critical systems and networks;
- A homeland security strategy to manage the urgent and growing risk of biological threats and hazards;
- A risk segmentation approach to securing and managing flows of people and goods; and
- A new framework for strengthening mission execution through public-private partnerships.

Beyond these strategic priorities, this review also highlights ongoing areas of priority and emphasis—countering nuclear threats, strengthening our national immigration system, and enhancing national resilience—based on key aspects of the security environment and policy priorities for homeland security.

Together, the strategic shifts and areas of renewed emphasis position DHS and our partners to address those threats and hazards that pose the most strategically significant risk to the Nation. Much work remains to be done to translate these strategies and priorities into action, including a DHS Strategic Plan that specifies necessary capabilities and associated investments, as well as focused efforts to enhance departmental management and improve workforce morale. We must all play a role—and through the commitment of each, we will secure the Nation for all.
APPENDIX A: HOMELAND SECURITY ROLES AND RESPONSIBILITIES

Homeland security spans the authorities and responsibilities of federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and private citizens and communities. For this reason, coordination and cooperation are essential to successfully carrying out and accomplishing the homeland security missions. This Appendix highlights key roles and responsibilities of the many homeland security partners and stakeholders. Nothing in this report alters, or impedes the ability to carry out, the authorities or missions of federal departments and agencies to perform their responsibilities or priorities under law.

- The President of the United States is the Commander in Chief and the leader of the Executive Branch of the Federal Government. The President, through the Homeland Security and National Security Councils and the National Security Council staff, provides overall homeland security policy direction and coordination.

- The Department of Homeland Security (DHS) is the federal agency defined by statute as charged with homeland security: preventing terrorism and enhancing security; securing and managing our borders; enforcing and administering our immigration laws; strengthening cyberspace and critical infrastructure; and strengthening national preparedness and resilience to disasters. The Secretary of Homeland Security is responsible for coordinating the domestic all-hazards preparedness efforts of all executive departments and agencies, in consultation with state, local, tribal, and territorial governments, nongovernmental organizations, private-sector partners, and the general public. Preparedness efforts include those actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats and hazards that pose the greatest risk to the security and resilience of the Nation. DHS includes U.S. Customs & Border Protection, U.S. Citizenship & Immigration Services, U.S. Coast Guard, Federal Emergency Management Agency, U.S. Immigration & Customs Enforcement, U.S. Secret Service, and Transportation Security Administration. DHS is the coordinating agency for multiple Emergency Support Functions under the National Response Framework (see Figure A-1). In particular, with respect to its responsibilities regarding safeguarding and security cyberspace:

  ◆ To better manage and facilitate cybersecurity information sharing efforts, analysis, and incident response activities, the Department operates the
National Cybersecurity and Communications Integration Center, an around-the-clock center where key government, private sector, and international partners all work together. The National Cybersecurity and Communications Integration Center serves as a focal point for coordinating cybersecurity information sharing with the private sector; provides technical assistance, onsite analysis, mitigation support, and assessment assistance to cyber-attack victims, as well as situational awareness capability that includes integrated, actionable information about emerging trends, imminent threats, and the status of incidents that may impact critical infrastructure; and coordinates the national response to significant cyber incidents affecting critical infrastructure.

DHS, through U.S. Immigration and Customs Enforcement Homeland Security Investigations, operates the Cyber Crime Center, which is responsible for providing domestic and international training; and the support, coordination and de-confliction of cyber investigations related to online economic crime, digital theft of export controlled data, digital theft of intellectual property and online child exploitation investigations. The U.S. Secret Service leads a network of Electronic Crimes Task Forces to bring together federal, state, and local law enforcement, prosecutors, private industry, and academia for the common purpose of preventing, detecting, mitigating, and investigating various forms of malicious cyber activity.

The Department of Justice (DOJ), led by the Attorney General, is responsible for prosecution of federal crimes. The Attorney General has lead responsibility for criminal investigation of terrorist acts or threats within the United States and its territories, as well as for related intelligence collection activities within the United States. The Attorney General, generally acting through the Director of the Federal Bureau of Investigation (FBI), in cooperation with other departments and agencies engaged in activities to protect national security, coordinates the activities of the law enforcement community to detect, prevent, preempt, and disrupt terrorist threats or incidents against the United States. DOJ approves state governor requests for personnel and other federal law enforcement support under the Emergency Federal Law Enforcement Assistance Act. DOJ supports the National Health Security Strategy and it is a member of the Mitigation Framework Leadership Group established under the National Mitigation Framework. In addition, DOJ is responsible for Emergency Support Function #13 (Public Safety and Security). In particular:
The mission of the FBI is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners; and to perform these responsibilities in a manner that is responsive to the needs of the public and is faithful to the Constitution of the United States. The FBI, primarily through Joint Terrorism Task Forces, has lead responsibility for the receipt and resolution of suspicious activity reporting of terrorist activities or acts in preparation of terrorist activities. The Attorney General, acting through the FBI Director, has primary responsibility for searching for, finding, and neutralizing weapons of mass destruction within the United States and its territories. As part of its efforts to investigate and disrupt cyber crime and national security cyber threats, the FBI is also responsible for operating the National Cyber Investigative Joint Task Force, a multi-agency national focal point with representation from intelligence, law enforcement, and military agencies to coordinate, integrate, and share information related to cyber threat investigations.

DOJ deconflicts federal criminal investigations through several organizations, including the International Organized Crime Intelligence and Operations Center, the Organized Crime Drug Enforcement Task Force Fusion Center. The International Organized Crime Intelligence and Operations Center is a multi-agency intelligence center whose mission is to significantly disrupt and dismantle those international criminal organizations posing the greatest threat to the United States, and to coordinate the resulting multi-jurisdictional investigations and prosecutions. The Organized Crime Drug Enforcement Task Force Fusion Center is a multi-agency intelligence center designed to produce actionable intelligence products to support the field. The Center’s unique capability includes cross-agency integration and analysis of data to develop products that are disseminated through the multi-agency Special Operations Division for further de-confliction before transmission to the field. All Organized Crime Drug Enforcement Task Force Fusion Center member agencies receive products, including the Task Force’s Co-Located Strike Forces.

The Department of State is the lead U.S. foreign affairs agency, and the Secretary of State is the President’s principal foreign policy advisor. The Department develops and
implements policies to advance U.S. objectives and interests in shaping a freer, more secure, and more prosperous world. The Department also supports the foreign affairs activities of other U.S. Government entities and works with international partner nations and regional and multilateral organizations to protect the U.S. homeland and U.S. interests and citizens abroad. The Department also provides an array of important services to U.S. citizens and to foreigners seeking to visit or immigrate to the United States. The Department supports the National Health Security Strategy and is the coordinating agency for the International Coordination Support Annex under the National Response Framework.

- The **Department of Defense’s (DOD)** military services, defense agencies, and geographic and functional commands protect the population of the United States and its territories, as well as the critical defense infrastructure, against external threats and aggression. DOD defends the Nation from attack; gathers foreign cyber threat intelligence and determines attribution; secures national security and military systems; supports national cyber incident protection, prevention, mitigation, and recovery; and investigates cybercrimes under military jurisdictions. DOD also provides support to civil authorities at the direction of the Secretary of Defense or the President when the capabilities of state, local, tribal, and territorial authorities to respond effectively to an event are overwhelmed. DOD is the lead coordinator for Emergency Support Function #3 (Public Works and Engineering) through the U.S. Army Corps of Engineers and provides support to the other Emergency Support Functions as directed.

  - DOD accomplishes its cybersecurity operational roles and responsibilities as part of the Federal Cybersecurity Operations Team through the CYBERCOM Joint Operations Center, the National Security Agency/Central Security Service Threat Operations Center, the Defense Cyber Crime Center, and the Defense Information Systems Agency Command Center, in coordination with the cybersecurity operations centers operated by DHS and DOJ.

- The **Department of Health and Human Services (HHS)** leads the coordination of all functions relevant to Public Health Emergency Preparedness and Disaster Medical Response. HHS incorporates steady-state and incident-specific activities as described in the National Health Security Strategy. HHS serves as a member of the Mitigation Framework Leadership Group, the coordinating and primary agency for the Public Health and Medical Services Emergency Support Function, the coordinating agency for
the Health and Social Services Recovery Support Function, and a primary agency for the Community Planning and Capacity Building Recovery Support Function.

- The **Department of the Treasury** works to safeguard the U.S. financial system, combat financial crimes, and cut off financial support to terrorists, weapons of mass destruction proliferators, drug traffickers, and other threats to the national security, foreign policy, or economy of the United States. Treasury is a primary agency for the Economic Recovery Support Function.

- The **Department of Agriculture (USDA)** provides leadership on food, agriculture, natural resources, rural development, and related issues based on sound public policy, the best available science, and efficient management. The Department works with private land owners to build more resilient agricultural systems and healthier forest to reduce the risk of wildfire, insects, and disease. The USDA is a member of the Emergency Support Function Leadership Group, Recovery Support Function Leadership Group, and Mitigation Framework Leadership Group, the coordinator and primary agency for the Firefighting Emergency Support Function and Agriculture and Natural Resources Emergency Support Function, and primary or support agency for all six Recovery Support Functions.

- **Office of the Director of National Intelligence (ODNI).** The Director of National Intelligence serves as the head of the Intelligence Community, acts as the principal advisor to the President for intelligence matters relating to national security, and oversees and directs implementation of the National Intelligence Program. In addition to intelligence community elements with specific homeland security missions, ODNI maintains a number of mission and support centers that provide unique capabilities for homeland security partners, including the National Counterterrorism Center and National Counterproliferation Center.

- The **Department of Commerce** promotes job creation, economic growth, sustainable development, and improved standards of living for all Americans. The Department of Commerce is a member of the Mitigation Framework Leadership Group and the coordinating agency and a primary agency for the Economic Recovery Support Function.

- The **Department of Education** oversees discretionary grants and technical assistance to help schools plan for and respond to emergencies that disrupt teaching and
The Department of Education supports the National Health Security Strategy and is a primary agency for the Health and Social Services Recovery Support Function.

- The Department of Energy (DOE) maintains stewardship of vital national security capabilities, from nuclear weapons to leading-edge research and development programs. DOE is the coordinating and primary agency for the Energy Emergency Support Function, is a member of the Mitigation Framework Leadership Group, and a primary agency for the Infrastructure Systems Recovery Support Function.

- The Environmental Protection Agency (EPA) is charged with protecting human health and the environment. EPA is a member of the Mitigation Framework Leadership Group, a primary agency for the Oil and Hazardous Materials Response Emergency Support Function, and a primary agency for the Natural and Cultural Resources and Health and Social Services Recovery Support Functions. EPA also carries out critical activities, as directed by Homeland Security Presidential Directive 10 and the National Response Framework, as it relates to decontamination.

- The Department of Housing and Urban Development is the coordinator and primary agency for the Housing Recovery Support Function and a member of the Mitigation Framework Leadership Group.

- The Department of the Interior (DOI) develops policies and procedures for all types of hazards and emergencies that impact Federal lands, facilities, infrastructure, and resources; tribal lands; and insular areas. DOI is also a member of the Mitigation Framework Leadership Group, a primary agency for the Search and Rescue Emergency Support Function, the coordinating agency and a primary agency for the Natural and Cultural Resources Recovery Support Function, and a primary agency for the Health and Social Services Recovery Support Function.

- The Department of Transportation (DOT) collaborates with DHS on all matters relating to transportation security and the security and resilience of transportation infrastructure and in regulating the transportation of hazardous materials by all modes (including pipelines). DOT supports the National Health Security Strategy and serves as a member of the Mitigation Framework Leadership Group, the coordinating agency for the Transportation Emergency Support Function, and a primary agency for the Infrastructure Systems Recovery Support Function.
The General Services Administration is a member of the Mitigation Framework Leadership Group.

The Department of Labor supports the National Health Security Strategy and is a primary agency for the Economic and Health and Social Services Recovery Support Functions. The Department of Labor/Occupational Safety and Health Administration is the Coordinating Agency for the Worker Safety and Health Support Annex under the National Response Framework.

The Department of Veteran's Affairs is a primary agency for the Health and Social Services Recovery Support Function.

The Small Business Administration is a member of the Mitigation Framework Leadership Group and a primary agency for the Economic Recovery Support Function.

Other Federal Agencies contribute to the homeland security mission in a variety of ways. This includes agencies responsible for either supporting efforts to assure a resilient homeland or collaborating with the departments and agencies noted above in their efforts to secure the homeland.

The American Red Cross is chartered by Congress to provide relief to survivors of disasters and help people prevent, prepare for, and respond to emergencies.

In addition to the roles and responsibilities specified above, Table A-1 identifies the coordinating and primary agencies for each of the Emergency Support Functions under the National Response Framework. The Emergency Support Functions are the primary federal coordinating structures for delivering response core capabilities established in the National Preparedness Goal.
<table>
<thead>
<tr>
<th>ESF #</th>
<th>ESF</th>
<th>ESF Coordinator</th>
<th>Primary Agency</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Transportation</td>
<td>Department of Transportation</td>
<td>Department of Transportation</td>
</tr>
<tr>
<td>2</td>
<td>Communications</td>
<td>DHS/National Protection and Programs/Cybersecurity and Communications/National Communications System</td>
<td>DHS/National Communications System DHS/FEMA</td>
</tr>
<tr>
<td>3</td>
<td>Public Works and Engineering</td>
<td>Department of Defense/U.S. Army Corps of Engineers</td>
<td>Department of Defense/U.S. Army Corps of Engineers</td>
</tr>
<tr>
<td>4</td>
<td>Firefighting</td>
<td>Department of Agriculture/Forest Service, DHS/FEMA</td>
<td>Department of Agriculture/Forest Service</td>
</tr>
<tr>
<td>5</td>
<td>Information and Planning</td>
<td>DHS/FEMA</td>
<td>DHS/FEMA</td>
</tr>
<tr>
<td>6</td>
<td>Mass Care, Emergency Assistance, Temporary Housing, and Human Services</td>
<td>DHS/FEMA</td>
<td>DHS/FEMA, American Red Cross</td>
</tr>
<tr>
<td>7</td>
<td>Logistics</td>
<td>General Services Administration, DHS/FEMA</td>
<td>General Services Administration, DHS/FEMA</td>
</tr>
<tr>
<td>8</td>
<td>Public Health and Medical Services</td>
<td>Department of Health and Human Services</td>
<td>Department of Health and Human Services</td>
</tr>
<tr>
<td>9</td>
<td>Search and Rescue</td>
<td>DHS/FEMA</td>
<td>DHS/FEMA, DHS/U.S. Coast Guard, DHS/Customs and Border Protection, Department of the Interior/National Park Service, Department of Defense</td>
</tr>
<tr>
<td>10</td>
<td>Oil and Hazardous Materials Response</td>
<td>Environmental Protection Agency</td>
<td>Environmental Protection Agency, DHS/ U.S. Coast Guard</td>
</tr>
<tr>
<td>11</td>
<td>Agriculture and Natural Resources</td>
<td>Department of Agriculture</td>
<td>Department of Agriculture, Department of the Interior</td>
</tr>
<tr>
<td>12</td>
<td>Energy</td>
<td>Department of Energy</td>
<td>Department of Energy</td>
</tr>
<tr>
<td>13</td>
<td>Public Safety and Security</td>
<td>Department of Justice/ Bureau of Alcohol, Tobacco, Firearms, and Explosives</td>
<td>Department of Justice/Bureau of Alcohol, Tobacco, Firearms, and Explosives</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>Superseded by National Disaster Recovery Framework</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>External Affairs</td>
<td>DHS</td>
<td>DHS/FEMA</td>
</tr>
</tbody>
</table>
In addition to the roles and responsibilities of federal departments and agencies, other homeland security participants include the following:

- **Private Sector Entities**, including businesses, industries, private schools and universities are integral parts of the community, and they play a wide range of critical roles. The majority of the Nation’s infrastructure is owned and operated by private sector entities. They take action to align relevant planning, training, exercising, risk management and investments in security as a necessary component of prudent business planning and operations. During times of disaster, private sector partners provide response resources—including specialized teams, essential services, equipment, and advanced technologies—through public-private emergency plans/partnerships, or mutual aid and assistance agreements, or in response to requests from government and from nongovernmental-volunteer initiatives. In addition, the private sector has a role in building community resiliency by preparing for, responding to, and recovering from emergencies affecting their businesses.

- **Governors** are responsible for overseeing their state’s threat prevention activities as well the state’s response to any emergency or disaster, and take an active role in ensuring that other state officials and agencies address the range of homeland security threats, hazards, and challenges. During an emergency, governors will play a number of roles, to include serving as the state’s chief communicator and primary source of information on the scope of the disaster, the need for evacuations, and the availability of assistance. Governors are commanders of their National Guards and are able to activate them to assist under state active duty during a disaster, and also retain command over their National Guard under Title 32 status. During a disaster, governors also will need to make decisions regarding the declaration of emergencies or disasters, requests for mutual aid, and calls for federal assistance.

- **State and Territorial Governments** supplement the activities of cities, counties, and intrastate regions. States administer federal homeland security grants (in certain grant programs) to local and tribal governments, allocating key resources to bolster their prevention and preparedness capabilities. State agencies conduct law enforcement and security activities, protect the governor and other executive leadership, and administer state programs that address the range of homeland security threats, hazards, and challenges. State government officials lead statewide disaster and mitigation planning. During response, states coordinate resources and capabilities throughout the state and are responsible for requesting and obtaining resources and capabilities from surrounding states. States often mobilize these
substantive resources and capabilities to supplement the local efforts before, during, and after incidents.

- **Tribal Leaders** are responsible for the public safety and welfare of their membership. They can serve as both key decision makers and trusted sources of public information during incidents.

- **Tribal Governments**, which have a special status under federal laws and treaties, ensure the provision of essential services to members within their communities, and are responsible for developing emergency response and mitigation plans. Tribal governments may coordinate resources and seek assistance from neighboring jurisdictions, states, and the Federal Government. Depending on location, land base, and resources, tribal governments provide law enforcement, fire, and emergency services as well as public safety to their members. During a disaster, tribal governments make decisions regarding whether to request a Presidential emergency or major disaster declaration independent of the state within which the tribal lands are located.

- **Mayors and Other Local Elected and Appointed Officials** are responsible for ensuring the public safety and welfare of their residents, serving as their jurisdiction’s chief communicator and a primary source of information for homeland security-related information, and are responsible for ensuring their governments are able to carry out emergency response activities. Officials serve as key decision makers and trusted sources of public information during incidents. In some states, elected officials such as sheriffs or judges also serve as emergency managers, search and rescue officials, and chief law enforcement officers.

- **Local Governments** are responsible for the public safety, security, health, and welfare of the people who live in their jurisdictions. Local governments promote the coordination of ongoing protection plans and the implementation of core capabilities, as well as engagement and information sharing with private sector entities, infrastructure owners and operators, and other jurisdictions and regional entities. Local governments also address unique geographical issues, dependencies and interdependencies among agencies and enterprises and, as necessary, the establishment of agreements for cross-jurisdictional and public-private coordination. Local governments provide front-line leadership for local law enforcement, fire, public safety, environmental response, public health, and emergency medical services for preventing, protecting, mitigating, and responding to all manner of hazards and
emergencies. They are also responsible for ensuring all citizens receive timely information in a variety of accessible formats and coordinate resources and capabilities during disasters with neighboring jurisdictions, nongovernmental organizations, the state, and the private sector.

- **Nongovernmental Organizations** provide sheltering, emergency food supplies, counseling services, and other vital services to support response and promote the recovery of disaster survivors. They often provide specialized services and advocacy that help individuals with special needs, including those with disabilities, and provide resettlement assistance and services to arriving refugees. They also provide for evacuation, rescue, shelter, and care of animals, including household pets and service animals. Nongovernmental organizations are key partners in preparedness activities to include response and recovery operations.

- **Communities** are unified groups that share goals, values, or purposes rather than geographic boundaries or jurisdictions. These groups may possess the knowledge and understanding of the threats and hazards, local response capabilities, and requirements within their jurisdictions and have the capacity to alert authorities of those emergencies, capabilities, or needs. During an incident these groups may be critical in passing along vital communications to individuals and families, and to supporting response activities in the initial stages of a crisis.

- **Individuals, Families, and Households** take protective actions and the basic steps to prepare themselves for emergencies, including understanding the threats and hazards that they may face, reducing hazards in and around their homes, preparing an emergency supply kit and household emergency plans (that include care for animals, including household pets and service animals), monitoring emergency communications, volunteering with established organizations, enrolling in training courses, and practicing what to do in an emergency. These preparedness activities help to strengthen community resilience and mitigate the impact of disasters. In addition, individual vigilance and awareness can help communities remain safer and bolster prevention efforts by contacting local law enforcement and sharing information within their communities.
APPENDIX B: PROCESS AND STAKEHOLDER ENGAGEMENT ACTIVITIES

Section 2401 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53, amends Title VII of the Homeland Security Act of 2002 to require the Secretary of Homeland Security to conduct a Quadrennial Homeland Security Review every four years beginning in 2009. In conducting the review, DHS is directed to consult with (1) the heads of other federal agencies, including the Attorney General, the Secretary of State, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of the Treasury, the Secretary of Agriculture, and the Director of National Intelligence; (2) key officials of the Department; and (3) other relevant governmental and nongovernmental entities, including state, local, tribal and territorial government officials, Members of Congress, private-sector representatives, academics, and other policy experts.

By articulating an enduring vision for and definition of homeland security, and establishing five homeland security missions, the first quadrennial review in 2010 answered the question, “What is homeland security?” Building on this foundation, the second quadrennial review identifies the necessary strategic shifts and areas of ongoing priority and renewed emphasis that will position DHS to successfully counter evolving threats and hazards, and keep our Nation safe. Pursuant to the legislative direction, the second review included two years of deliberate, rigorous analysis and substantive collaboration with partners at all levels of government and across the public and private sector.

REVIEW APPROACH: STRATEGY THROUGH ANALYSIS

The second Quadrennial Homeland Security Review included four phases: (1) preparation; (2) study and analysis; (3) writing and decision; and (4) rollout. The preparation phase, which took place in 2012 and early 2013, included a review of homeland security risks and the dynamic security environment, as well as preliminary updates to the goals within the homeland security missions. The study and analysis phase, which took place during the spring and summer of 2013, focused on deep dive studies and targeted analyses. The writing and decision phase, which took place in fall 2013 and early 2014, interrupted by the partial government shutdown in October 2013, aimed at reaching decisions on high-priority questions with interagency partners and external stakeholders. As with the first Quadrennial Homeland Security Review, substantive engagement and outreach across a wide variety of stakeholders were critical across all stages of the review. Roll-out culminates the engagement with the release of the second quadrennial review. As with the
first review, the Office of Policy (PLCY), through its Office of Strategy, Planning, Analysis & Risk, served as the executive agent for the second review.

**PREPARATION PHASE**

The Quadrennial Homeland Security Review preparation phase began in 2012 and focused on two primary efforts to prepare the Department to successfully execute the second review: (1) deeply examining the strategic environment, including threats and hazards, trends, future uncertainties, and strategic risk; and (2) reviewing, affirming, and where necessary updating the DHS missions and goals based on changes since the first quadrennial review. During this process, DHS developed a Homeland Security Strategic Environmental Assessment, which combined cross-cutting threat and hazard analysis with an examination of the changing risk environment through analysis of system relationships, trends, and future uncertainties. The result was insight into how strategic homeland security risk will likely evolve over time, and a clear sense of the threats and hazards that pose the most strategically significant risk to the Nation over the next five years. The Department also conducted a roles and missions review that affirmed the enduring nature
of the five core missions and the cross-cutting imperative to Mature and Strengthen Homeland Security.

STUDY AND ANALYSIS PHASE

Based on the preparation phase analyses and informed by conclusions about the areas that pose the most strategic significant risk, DHS leadership directed the following Quadrennial Homeland Security Review studies: (1) The Evolving Terrorism Threat; (2) Cybersecurity; (3) A Homeland Security Strategy for Countering Biological Threats and Hazards; (4) Securing and Expediting Flows of People and Goods; and (5) Governance in the Homeland Security Enterprise: The Public-Private Relationship. Several key areas of ongoing emphasis—Nuclear Terrorism Using an Improvised Nuclear Device, Immigration; and the National Preparedness System and the Whole Community Approach—were the subject of ongoing efforts pursuant to Congressional and Presidential direction and therefore were not explicitly studied in the quadrennial review process.

Each Quadrennial Homeland Security Review study involved a strategic review of the topic area, with on-going guidance and in-progress decisions from Departmental leadership. Each study group included a leader from PLCY’s Office of Strategy, Planning, Analysis, and Risk, and a dedicated group of senior managers and subject matter experts from across DHS. Each study followed a tailored analytic plan based on a common approach to strategy development and analysis. This common approach includes four sequential elements with associated analytic milestones and deliverables:

- **Lay the Foundations**—Departmental leadership provided guidance, defined priorities, and set expectations for each study, while study groups developed plans for engaging partners and stakeholders inside and outside DHS;

- **Define the Context**—each study framed the challenge, including understanding threat and risk today and making assumptions about the future given key trends and uncertainties, and specified desired end-states;

- **Develop Solutions**—each study defined key priorities or areas of emphasis to best address the challenge and meet desired outcomes; where applicable, studies considered alternatives that traded off cost, risk reduction, executability, and robustness against future uncertainty; and
- **Decide on an Approach**—each study worked through relevant criteria and results from analysis to reach conclusions and recommendations for leadership on strategic posture shifts and areas of ongoing or renewed emphasis.

**WRITING AND DECISION PHASE**

Study group recommendations were provided to DHS leadership through the Quadrennial Homeland Security Review Executive Steering Committee, a body of senior executives from all DHS directorates, Components, and offices, and a series of Deputy Component head meetings chaired by the Deputy Secretary. The Department initiated drafting of the Quadrennial Homeland Security Review Report once decisions were reached across all studies. Decisions were informed by input from interagency partners and homeland security communities of interest, as described in “Stakeholder Engagement,” below.

**ROLL-OUT PHASE**

The roll-out phase focuses on generating substantive dialogue with our partners and stakeholders, to include the public, on the future of the Nation’s homeland security. The ultimate goal for the second review is to foster discussion about Quadrennial Homeland Security Review conclusions across the broad range of homeland security partners and stakeholders, and to drive review conclusions into programs and budgets, major investments, and operations.

**STAKEHOLDER ENGAGEMENT**

Throughout the Quadrennial Homeland Security Review study process, DHS conducted extensive engagement with federal executive branch partners and Congress; state, local, tribal and territorial partners; the private sector; academics; and others. The primary goal of stakeholder engagement was to solicit stakeholder perspectives on studies and supporting analysis, and to incorporate that input into the second quadrennial review. Since the Quadrennial Homeland Security Review Terms of Reference directed that the second review be an enterprise-wide review, a thorough and accurate picture of the homeland security landscape, and robust participation from stakeholders across all aspects of the enterprise was required. Acquiring this input involved engaging a group of stakeholders that was broad enough to present perspectives from across the enterprise and possessed the subject matter expertise needed to inform the analytic studies. Our analytical efforts focused on reviewing, researching, and synthesizing existing literature and academic work on the study topics, in-person discussions with experts in the field, and
the participation of homeland security stakeholders.

Pursuant to the Quadrennial Homeland Security Review legislative mandate, the review engagement strategy sought input from three groups of stakeholders (see Figure B-2):

Figure B-2: DHS engaged three distinct stakeholder communities

DEPARTMENT OF HOMELAND SECURITY

Throughout the review, DHS employees at all levels were consulted and provided input. Each study lead convened a group of subject matter experts to shape and inform the analysis. An Executive Steering Committee of DHS Senior Executives guided the overarching narrative and presented decisions to DHS senior leadership through a series of Component Deputy Meetings:
**Study Groups:** In keeping with the inclusive approach of the review, more than 200 participants from across DHS Components and offices conducted each of the studies through standing working groups, led by a core group of analysts from PLCY’s Office of Strategy, Planning, Analysis, and Risk. The work of the DHS study group participants was supported by a team of subject-matter experts and research analysts from the Homeland Security Studies and Analysis Institute, one of the Department’s federally funded research and development centers. The study groups conducted their analysis over a 12-month period, with work products consistently shared using the online portals described in “Homeland Security Communities of Interest,” below.

**Executive Steering Committee:** A Steering Committee, chaired by the Assistant Secretary for Strategy, Planning, Analysis & Risk and made up of senior executive-level representatives of all DHS Components, met more than 25 times for coordination and consultation through the course of the review. The Steering Committee provided insight and suggestions, and shaped study group material for decision.

**DHS Senior Leadership Meetings:** The DHS Deputy Secretary hosted leadership meetings more than a dozen times throughout the review process, in order to shape the preferred approach of each study topic and to review final results. Final decisions on the recommendations reflected departmental acknowledgement of major themes around which the Quadrennial Homeland Security Review Report was written.

**FEDERAL PARTNERS**

Stakeholders across the Federal Government were consulted throughout the review process, culminating in a series of decisions that informed both policy and budget priorities. Federal partners received regular briefings and participated in discussions at key decision points during the review.

**Legislative Branch:** Staff-level briefings on Quadrennial Homeland Security Review progress were offered to all relevant committees on a variety of occasions, and provided to the House Committee on Homeland Security, the Senate Homeland Security and Governmental Affairs Committee, and the Senate Appropriations Committee. Additionally, key members and staff of relevant committees were invited to participate on the online engagement venues; several joined to monitor and participate in quadrennial review discussions. In discussions with congressional staff, their access to the ongoing online discussion was invaluable in understanding the process and results of the review. Chairman Michael McCaul (R-TX) and Ranking Member Bennie Thompson (D-MS) of the House Committee on Homeland Security also provided consolidated input to the process in...
a joint letter sent to the Department in December 2013.

**Executive Branch:** The Quadrennial Homeland Security Review team held regular synchronization briefings with executive branch staff to remain aligned with evolving presidential policy decisions, budget priorities, and national security concerns, and to enable mutual awareness of the progress and direction of the review.

- **Interagency Policy Process:** Input from federal partners was coordinated through meetings under the National Security Council (NSC) structure. Sub-Interagency Policy Committees were convened for interagency engagement and a series of Interagency Policy Committee-level briefings were used to socialize quadrennial review progress and decisions. Sub-Interagency Policy Committees were set up specifically for the Quadrennial Homeland Security Review studies on a Homeland Security Strategy for Countering Biological Threats and Hazards, Securing and Managing Flows of People and Goods, and Governance in the Homeland Security Enterprise: The Public-Private Relationship.

- **Direct Engagement with other Agencies:** In order to fulfill the requirement of consulting with other federal agencies, DHS engaged in interagency coordination through the NSC staff as well as direct bilateral meetings with interagency partners to receive interdepartmental expertise and coordinate strategy. These direct departmental meetings included discussions with the Departments of Defense, Justice, State, Health and Human Services, Veterans Affairs, Agriculture, and Treasury, as well as the Environmental Protection Agency, and the Internal Revenue Service.

- **Direct Engagement with the Executive Office of the President:** DHS engaged directly with various offices and policy council staff of the Executive Office of the President, including the NSC staff, staff from the Office of Management and Budget (OMB), and the Office of National Drug Control Policy. DHS held nearly two dozen meetings with senior NSC staff to help drive consensus throughout the strategic review process and ensured interagency coordination on key issues. DHS met monthly with OMB staff to update them on progress of the Quadrennial Homeland Security Review and the FY14-18 DHS Strategic Plan. DHS also consulted with the Office of National Drug Control Policy to confirm data related to securing and expediting flows of people and goods, and the Domestic Policy Council staff for insight on topics related to immigration.
HOMELAND SECURITY COMMUNITIES OF INTEREST

Outreach efforts focused on a cross-section of homeland security stakeholders. In order to reach the widest swath of homeland security practitioners and experts using available resources, pre-existing online venues were used as a primary mechanism for engagement. Two sites—the Quadrennial Homeland Security Review Community of Practice hosted through DHS Science and Technology’s FirstResponder.gov Communities of Practice and the IdeaScale site managed by the DHS Office of Public Affairs—served as the primary interface between quadrennial review study teams and homeland security stakeholders.

In June 2013 the Secretary invited more than 200 organizations and their members, representing all facets of homeland security, to join the Quadrennial Homeland Security Review Community of Practice, which was linked to the Quadrennial Homeland Security Review IdeaScale site. This invitation garnered dynamic and enthusiastic participation throughout the entire review process from subject matter experts in the field. Their essential insights strengthened and supported the review, providing a holistic understanding of the realities of homeland security.

While the engagement process aimed to receive extensive stakeholder input, it also sought informed expertise that could be used for quadrennial review studies and analysis. To that end, the Quadrennial Homeland Security Review team reached out to:

- Hundreds of key organizations representing state, local, tribal, and territorial elected and appointed officials, and the national associations, organizations, and affiliates that represent them, the private sector, and non-profit organizations;

- Tens of thousands of practitioners through homeland security listservs managed by FEMA, DHS Intergovernmental Affairs, the Naval Postgraduate School, and the First Responder Community of Practice, among others;

<table>
<thead>
<tr>
<th>Stakeholder Group</th>
<th>Percentage of Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>State, Local, Tribal, Territorial Employee</td>
<td>27%</td>
</tr>
<tr>
<td>Private Sector</td>
<td>25%</td>
</tr>
<tr>
<td>Nongovernmental Organization/Non-profit</td>
<td>6%</td>
</tr>
<tr>
<td>Academia</td>
<td>9%</td>
</tr>
<tr>
<td>Federal Government</td>
<td>32%</td>
</tr>
</tbody>
</table>

Figure B-3: Stakeholder participation in IdeaScale
Hundreds of Federal Advisory Committee Act Committee members;

Several international partners with interest in homeland security topics; and

Individual organizations and experts closely related to quadrennial review study topics.

These stakeholders were targeted for extensive involvement throughout the Quadrennial Homeland Security Review study process. Study groups developed IdeaScale and Community of Practice engagement topics directly related to their analysis and stakeholders were invited to provide their thoughts and ideas. Between the two online venues, more than 2,000 unique stakeholders registered to provide their perspectives and insights, yielding thousands of comments, more than 100 source documents, and more than 10,000 votes. Stakeholders from across disciplines and from every state and several territories and tribal nations participated in these engagements. This focused and substantive input was used to inform study group analysis and helped shape the final Quadrennial Homeland Security Review Report.

To supplement this online engagement, study groups held a series of briefings and forums to solicit input and socialize the quadrennial review process with members of DHS Advisory Committees. Following the 2010 review, the Government Accountability Office (GAO) noted that the review did not fully utilize Federal Advisory Committee Act groups due to a number of limitations. Specifically, it was suggested by GAO that as the limitations of Federal Advisory Committee Act “significantly reduced the role that nonfederal stakeholders played in the [Quadrennial Homeland Security Review]...addressing the [Federal Advisory Committee Act] requirements and including appropriate [Federal Advisory Committee Act]-compliant groups with a broader range of academics and others could have affected the outcome of the study group’s deliberations.”

In order to remediate this issue, PLCY’s Office of Strategy, Planning, Analysis, and Risk held eight Quadrennial Homeland Security Review Forums to engage with members of DHS Federal Advisory Committee Act committees between April and December 2013. The forums allowed the Department to engage DHS’s advisory committee members as individual stakeholders with relevant expertise in focused briefings. These forums did not function as Advisory Committee meetings, as the members who attended were not solicited for consensus advice or recommendations, did not speak on behalf of the Committees, and each forum consisted of different members from across the Department’s Advisory Committees. When individual DHS Advisory Committees requested specific quadrennial review briefings, staff from PLCY’s Office of Strategy, Planning, Analysis, and Risk provided those briefings at the
committees’ regularly-scheduled and publicly-noticed meetings. DHS also engaged with specific organizations to host review-related activities, including a forum on public-private partnerships hosted by the U.S. Chamber of Commerce and a public-private partnerships tabletop exercise held in conjunction with Business Executives for National Security.

1 In January 2014, the Assistant to the President for National Security Affairs changed the name of the integrated National Security Council and Homeland Security Council staff from the National Security Staff (NSS) to the National Security Council (NSC) staff. This appendix refers to the NSC staff, although during the conduct of the review the staff was referred to in QHSR preparatory documents as the NSS.

Global Risks 2015, 10th Edition is published by the World Economic Forum within the framework of The Global Competitiveness and Benchmarking Network.

The information in this report, or on which this report is based, has been obtained from sources that the authors believe to be reliable and accurate. However, it has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties. In addition, the statements in this report may provide current expectations of future events based on certain assumptions and may include statements that do not directly relate to a historical or current fact. These statements involve known and unknown risks, uncertainties and other factors which are not exhaustive. Readers are cautioned not to place undue reliance on these statements. The companies contributing to this report undertake no obligation to publicly revise or update any statements, whether as a result of new information, future events or otherwise, and they shall in no event be liable for any loss or damage arising in connection with the use of the information in this report.

World Economic Forum
Geneva

World Economic Forum®

© 2015 – All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

REF: 090115

This report and an interactive data platform are available at www.weforum.org/risks.
Figure 1: The Global Risks Landscape 2015

Top 10 risks in terms of Likelihood
1. Interstate conflict
2. Extreme weather events
3. Failure of national governance
4. State collapse or crisis
5. Unemployment or underemployment
6. Natural catastrophes
7. Failure of climate-change adaptation
8. Water crises
9. Data fraud or theft
10. Cyber attacks

Top 10 risks in terms of Impact
1. Water crises
2. Spread of infectious diseases
3. Weapons of mass destruction
4. Interstate conflict
5. Failure of climate-change adaptation
6. Energy price shock
7. Critical information infrastructure breakdown
8. Fiscal crises
9. Unemployment or underemployment
10. Biodiversity loss and ecosystem collapse

Source: Global Risks Perception Survey 2014.
Note: Survey respondents were asked to assess the likelihood and impact of the individual risks on a scale of 1 to 7, 1 representing a risk that is not likely to happen or have impact, and 7 a risk very likely to occur and with massive and devastating impacts. See Appendix B for more details. To ensure legibility, the names of the global risks are abbreviated. Also see Appendix A for the full name and description.
### Table A: Global Risks 2015

<table>
<thead>
<tr>
<th>Economic</th>
<th>Environmental</th>
<th>Geopolitical</th>
<th>Societal</th>
<th>Technological</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset bubble in a major economy</td>
<td>Asset bubble in a major economy</td>
<td>Asset bubble in a major economy</td>
<td>Asset bubble in a major economy</td>
<td>Asset bubble in a major economy</td>
</tr>
<tr>
<td>Deflation in a major economy</td>
<td>Deflation in a major economy</td>
<td>Deflation in a major economy</td>
<td>Deflation in a major economy</td>
<td>Deflation in a major economy</td>
</tr>
<tr>
<td>Energy price shock to the global economy</td>
<td>Energy price shock to the global economy</td>
<td>Energy price shock to the global economy</td>
<td>Energy price shock to the global economy</td>
<td>Energy price shock to the global economy</td>
</tr>
<tr>
<td>Failure of a major financial mechanism or institution</td>
<td>Failure of a major financial mechanism or institution</td>
<td>Failure of a major financial mechanism or institution</td>
<td>Failure of a major financial mechanism or institution</td>
<td>Failure of a major financial mechanism or institution</td>
</tr>
<tr>
<td>Failure/shortfall of critical infrastructure</td>
<td>Failure/shortfall of critical infrastructure</td>
<td>Failure/shortfall of critical infrastructure</td>
<td>Failure/shortfall of critical infrastructure</td>
<td>Failure/shortfall of critical infrastructure</td>
</tr>
<tr>
<td>Fiscal crises in key economies</td>
<td>Fiscal crises in key economies</td>
<td>Fiscal crises in key economies</td>
<td>Fiscal crises in key economies</td>
<td>Fiscal crises in key economies</td>
</tr>
<tr>
<td>High structural unemployment or underemployment</td>
<td>High structural unemployment or underemployment</td>
<td>High structural unemployment or underemployment</td>
<td>High structural unemployment or underemployment</td>
<td>High structural unemployment or underemployment</td>
</tr>
<tr>
<td>Unmanageable inflation</td>
<td>Unmanageable inflation</td>
<td>Unmanageable inflation</td>
<td>Unmanageable inflation</td>
<td>Unmanageable inflation</td>
</tr>
<tr>
<td>Extreme weather events (e.g. floods, storms, etc.)</td>
<td>Extreme weather events (e.g. floods, storms, etc.)</td>
<td>Extreme weather events (e.g. floods, storms, etc.)</td>
<td>Extreme weather events (e.g. floods, storms, etc.)</td>
<td>Extreme weather events (e.g. floods, storms, etc.)</td>
</tr>
<tr>
<td>Failure of climate-change adaptation</td>
<td>Failure of climate-change adaptation</td>
<td>Failure of climate-change adaptation</td>
<td>Failure of climate-change adaptation</td>
<td>Failure of climate-change adaptation</td>
</tr>
<tr>
<td>Major biodiversity loss and ecosystem collapse (land or ocean)</td>
<td>Major biodiversity loss and ecosystem collapse (land or ocean)</td>
<td>Major biodiversity loss and ecosystem collapse (land or ocean)</td>
<td>Major biodiversity loss and ecosystem collapse (land or ocean)</td>
<td>Major biodiversity loss and ecosystem collapse (land or ocean)</td>
</tr>
<tr>
<td>Major natural catastrophes (e.g. earthquake, tsunami, volcanic eruption, geomagnetic storms)</td>
<td>Major natural catastrophes (e.g. earthquake, tsunami, volcanic eruption, geomagnetic storms)</td>
<td>Major natural catastrophes (e.g. earthquake, tsunami, volcanic eruption, geomagnetic storms)</td>
<td>Major natural catastrophes (e.g. earthquake, tsunami, volcanic eruption, geomagnetic storms)</td>
<td>Major natural catastrophes (e.g. earthquake, tsunami, volcanic eruption, geomagnetic storms)</td>
</tr>
<tr>
<td>Man-made environmental catastrophes (e.g. oil spill, radioactive contamination, etc.)</td>
<td>Man-made environmental catastrophes (e.g. oil spill, radioactive contamination, etc.)</td>
<td>Man-made environmental catastrophes (e.g. oil spill, radioactive contamination, etc.)</td>
<td>Man-made environmental catastrophes (e.g. oil spill, radioactive contamination, etc.)</td>
<td>Man-made environmental catastrophes (e.g. oil spill, radioactive contamination, etc.)</td>
</tr>
<tr>
<td>Failure of national governance (e.g. corruption, illicit trade, organized crime, impunity, political deadlock, etc.)</td>
<td>Failure of national governance (e.g. corruption, illicit trade, organized crime, impunity, political deadlock, etc.)</td>
<td>Failure of national governance (e.g. corruption, illicit trade, organized crime, impunity, political deadlock, etc.)</td>
<td>Failure of national governance (e.g. corruption, illicit trade, organized crime, impunity, political deadlock, etc.)</td>
<td>Failure of national governance (e.g. corruption, illicit trade, organized crime, impunity, political deadlock, etc.)</td>
</tr>
<tr>
<td>Interstate conflict with regional consequences</td>
<td>Interstate conflict with regional consequences</td>
<td>Interstate conflict with regional consequences</td>
<td>Interstate conflict with regional consequences</td>
<td>Interstate conflict with regional consequences</td>
</tr>
<tr>
<td>Large-scale terrorist attacks</td>
<td>Large-scale terrorist attacks</td>
<td>Large-scale terrorist attacks</td>
<td>Large-scale terrorist attacks</td>
<td>Large-scale terrorist attacks</td>
</tr>
<tr>
<td>State collapse or crisis (e.g. civil conflict, military coup, failed states, etc.)</td>
<td>State collapse or crisis (e.g. civil conflict, military coup, failed states, etc.)</td>
<td>State collapse or crisis (e.g. civil conflict, military coup, failed states, etc.)</td>
<td>State collapse or crisis (e.g. civil conflict, military coup, failed states, etc.)</td>
<td>State collapse or crisis (e.g. civil conflict, military coup, failed states, etc.)</td>
</tr>
<tr>
<td>Weapons of mass destruction</td>
<td>Weapons of mass destruction</td>
<td>Weapons of mass destruction</td>
<td>Weapons of mass destruction</td>
<td>Weapons of mass destruction</td>
</tr>
<tr>
<td>Failure of urban planning</td>
<td>Failure of urban planning</td>
<td>Failure of urban planning</td>
<td>Failure of urban planning</td>
<td>Failure of urban planning</td>
</tr>
<tr>
<td>Food crises</td>
<td>Food crises</td>
<td>Food crises</td>
<td>Food crises</td>
<td>Food crises</td>
</tr>
<tr>
<td>Large-scale involuntary migration</td>
<td>Large-scale involuntary migration</td>
<td>Large-scale involuntary migration</td>
<td>Large-scale involuntary migration</td>
<td>Large-scale involuntary migration</td>
</tr>
<tr>
<td>Profound social instability</td>
<td>Profound social instability</td>
<td>Profound social instability</td>
<td>Profound social instability</td>
<td>Profound social instability</td>
</tr>
<tr>
<td>Rapid and massive spread of infectious diseases</td>
<td>Rapid and massive spread of infectious diseases</td>
<td>Rapid and massive spread of infectious diseases</td>
<td>Rapid and massive spread of infectious diseases</td>
<td>Rapid and massive spread of infectious diseases</td>
</tr>
<tr>
<td>Water crises</td>
<td>Water crises</td>
<td>Water crises</td>
<td>Water crises</td>
<td>Water crises</td>
</tr>
<tr>
<td>Breakdown of critical information infrastructure and networks</td>
<td>Breakdown of critical information infrastructure and networks</td>
<td>Breakdown of critical information infrastructure and networks</td>
<td>Breakdown of critical information infrastructure and networks</td>
<td>Breakdown of critical information infrastructure and networks</td>
</tr>
<tr>
<td>Large-scale cyber attacks</td>
<td>Large-scale cyber attacks</td>
<td>Large-scale cyber attacks</td>
<td>Large-scale cyber attacks</td>
<td>Large-scale cyber attacks</td>
</tr>
<tr>
<td>Massive incident of data fraud/theft</td>
<td>Massive incident of data fraud/theft</td>
<td>Massive incident of data fraud/theft</td>
<td>Massive incident of data fraud/theft</td>
<td>Massive incident of data fraud/theft</td>
</tr>
<tr>
<td>Massive and widespread misuse of technologies (e.g. 3D printing, artificial intelligence, geo-engineering, synthetic biology, etc.)</td>
<td>Massive and widespread misuse of technologies (e.g. 3D printing, artificial intelligence, geo-engineering, synthetic biology, etc.)</td>
<td>Massive and widespread misuse of technologies (e.g. 3D printing, artificial intelligence, geo-engineering, synthetic biology, etc.)</td>
<td>Massive and widespread misuse of technologies (e.g. 3D printing, artificial intelligence, geo-engineering, synthetic biology, etc.)</td>
<td>Massive and widespread misuse of technologies (e.g. 3D printing, artificial intelligence, geo-engineering, synthetic biology, etc.)</td>
</tr>
</tbody>
</table>

### Table B: Trends 2015

- Ageing population
- Climate change
- Environmental degradation
- Growing middle class in emerging economies
- Increasing national sentiment
- Increasing polarization of societies
- Rise of chronic diseases
- Rise of hyperconnectivity
- Rising geographic mobility
- Rising income disparity
- Shifts in power
- Urbanization
- Weakening of international governance
Profound social instability

Unemployment or underemployment

Interstate conflict

State collapse or crisis

Failure of climate-change adaptation

Fiscal crises

Biodiversity loss and ecosystem collapse

Failure of urban planning

Food crises

Extreme weather events

Rising geographic mobility

Urbanization

Environmental degradation

Failure of national governance

Rise of chronic diseases

Rise of hyperconnectivity

Weakening of international governance

Increasing national sentiment

Increasing polarization of societies

Shifts in power

Ageing population

Growing middle class in emerging economies

Asset bubble

Rise of hyperconnectivity

Rising income disparity

Environmental degradation

Data fraud or theft

Climate change

Rising income disparity

Asset bubble

Rise of hyperconnectivity

Environmental degradation

Data fraud or theft

Ageing population

Rising income disparity

Asset bubble

Data fraud or theft

Weakening of international governance

Shifts in power

Increasing national sentiment

Rising geographic mobility

Clustering of connections (‘weighted degree’)

Economic Risks

Environmental Risks

Geopolitical Risks

Societal Risks

Technological Risks

Trends

Source: Global Risks Perception Survey 2014.

Note: Survey respondents were asked to select between three and six trends and to identify for each the risk they believe is most interconnected. See Appendix B for more details. To ensure legibility, the names of the global risks are abbreviated. Also see Appendix A for the full name and description.
Figure 2: The Global Risks 2015 Interconnections Map

Source: Global Risks Perception Survey 2014.
Note: Survey respondents were asked to identify between three and six pairs of global risks they believe to be most interconnected. See Appendix B for more details. To ensure legibility, the names of the global risks are abbreviated. Also see Appendix A for the full name and description.
Global Risks 2015
10th Edition

Strategic Partners
Marsh & McLennan Companies
Zurich Insurance Group

Academic Advisers
National University of Singapore
Oxford Martin School, University of Oxford
Wharton Risk Management and Decision Processes Center, University of Pennsylvania
This 10th edition of the Global Risks report is published at a time of profound transformations to our global context. Ongoing political, economic, social, environmental and technological developments are challenging many of our underlying assumptions. Across every sector of society, decision-makers are struggling to cope with heightened complexity and uncertainty resulting from the world’s highly interconnected nature and the increasing speed of change.

Faster communication systems, closer trade and investment links, increasing physical mobility and enhanced access to information have combined to bind countries, economies and businesses more tightly together. In the coming decade – the time horizon of this report – our lives will be even more intensely shaped by transformative forces that are under way already. The effects of climate change are accelerating and the uncertainty about the global geopolitical context and the effects it will have on international collaboration will remain. At the same time, societies are increasingly under pressure from economic, political and social developments including rising income inequality, but also increasing national sentiment. Last but not least, new technologies, such as the Internet or emerging innovations will not bear fruit if regulatory mechanisms at the international and national levels cannot be agreed upon.

In a world where risks transcend borders and sectors, the motivations underlying the Global Risks report at its inception in 2005 – to shed light on global risks and help create a shared understanding of the most pressing issues, the ways they interconnect and their potential negative impacts – are more relevant than ever. The shared understanding of challenges is needed as a base for multistakeholder collaboration, which has seen increasing recognition as the most effective way to address global risks and build resilience against them. To further inspire action, in this year’s report we include a new section sharing examples of risk mitigation and resilience practices.

As in previous years, the report is based on the annual Global Risks Perception Survey, completed by almost 900 members of the World Economic Forum’s global multistakeholder community. This year’s report introduces a new distinction between risks and trends, which allows the highlighting of trends as an enlarged solution space to many possible risks. The report also presents deep-dive discussions of the risks posed by a resurgence of interlinked economic and geopolitical power plays, the rapid urbanization of the developing world and the exciting realm of emerging technologies, from synthetic biology to artificial intelligence.

The coming year offers unprecedented opportunities for much-needed collective action to address key global risks, such as the Sendai world conference on disaster risk reduction and the 2015 United Nations Climate Change Conference in Paris. As we mark the 10th anniversary of the report and highlight progress that has been achieved over the past decade, my hope remains that this work will contribute to the debate on how we think about global risks, mitigate them and strengthen resilience.

Klaus Schwab
Founder and Executive Chairman
World Economic Forum
Collaboration across countries, areas of expertise and stakeholder groups is necessary to effectively address global risks. As one of the flagship reports of the World Economic Forum, the Global Risks report has been a collaborative effort since its first edition in 2006. Produced within the World Economic Forum’s forward looking networked think tank, the Centre for Global Strategies, the report is able to draw on unique expertise available within the different communities and the knowledge networks of the World Economic Forum as well as within the organization as a whole.

The 2015 edition has established a Steering Board to provide strategic guidance as well as a high-level multistakeholder Advisory Board for advising on the methodology and the content of the report. The report’s corporate partners, academic advisors, and members of the Advisory Board contributed greatly to this endeavour. It also strongly builds on ongoing research, projects, debates and initiatives within the World Economic Forum. The insights presented here are the result of numerous discussions, consultations, and workshops and reflect the views of leaders from our various communities through the Global Risks Perception Survey.

With this in mind, I would like to thank our corporate report partners, Marsh & McLennan Companies and Zurich Insurance Group, represented on the Steering Board by John Drzik, President, Global Risk and Specialties, Marsh, and Axel Lehmann, Member, Group Chief Risk Officer, Zurich Insurance Group. Further, I am grateful to our academic advisers the National University of Singapore, Oxford Martin School at the University of Oxford and the Wharton Risk Management and Decision Processes Center at the University of Pennsylvania.

The report has also greatly benefited from the dedication and valuable guidance of the members of the Global Risks 2015 Advisory Board. Members are Rolf Alter, Organisation for Economic Co-operation and Development; Mario Blejer, Banco Hipotecario; Oliver Chen, Global Valuation, who represents the National University of Singapore; Megan Clark, Commonwealth Scientific and Industrial Research Organization; Marie-Valentine Florin, International Risk Governance Council; Julian Laird, Oxford Martin School; Pascal Lamry, Notre Europe – Jacques Delors Institute; Ursula von der Leyen, Federal Minister of Defence of Germany; Erwann Michel-Kerjan, the Wharton School, University of Pennsylvania; Moisés Naím, Carnegie Endowment for International Peace; Jonathan Ostry, International Monetary Fund; Manuel Pulgar-Vidal Otalora, Minister of Environment of Peru; Nouriel Roubini, New York University; Anders Sandberg, University of Oxford; Richard Smith-Bingham, Marsh & McLennan Companies; Michelle Tuveson, University of Cambridge; Margareta Wahlström, United Nations International Strategy for Disaster Reduction; and Steve Wilson, Zurich Insurance Group.

I am also grateful to Margareta Drzeniek Hanouz, Lead Economist and Head, Global Competitiveness and Risks, and the Global Risks 2015 project team members Ciara Browne, Jonathon Cini, Roberto Crotti, Attilio Di Battista, Gaëlle Dreyer, Caroline Galvan, Thierry Geiger, Tania Gutknecht and Cecilia Serin for their contributions to the report.

Last but not least, I would like to thank the respondents that completed the Global Risks Perception Survey.

Esben Barth Eide
Managing Director
and Member of the Managing Board
World Economic Forum
The 2015 edition of the Global Risks report completes a decade of highlighting the most significant long-term risks worldwide, drawing on the perspectives of experts and global decision-makers. Over that time, analysis has moved from risk identification to thinking through risk interconnections and the potentially cascading effects that result. Taking this effort one step further, this year’s report underscores potential causes as well as solutions to global risks. Not only do we set out a view on 28 global risks in the report’s traditional categories (economic, environmental, societal, geopolitical and technological) but also we consider the drivers of those risks in the form of 13 trends. In addition, we have selected initiatives for addressing significant challenges, which we hope will inspire collaboration among business, government and civil society communities.

Mapping Global Risks in 2015

The Global Risks Landscape, a map of the most likely and impactful global risks, puts forward that, 25 years after the fall of the Berlin Wall, “interstate conflict” is once again a foremost concern (see Table 1). However, 2015 differs markedly from the past, with rising technological risks, notably cyber attacks, and new economic realities, which remind us that geopolitical tensions present themselves in a very different world from before. Information flows instantly around the globe and emerging technologies have boosted the influence of new players and new types of warfare. At the same time, past warnings of potential environmental catastrophes have begun to be borne out, yet insufficient progress has been made – as reflected in the high concerns about failure of climate-change adaptation and looming water crises in this year’s report.

These multiple cross-cutting challenges can threaten social stability, perceived to be the issue most interconnected with other risks in 2015, and additionally aggravated by the legacy of the global economic crisis in the form of strained public finances and persistent unemployment. The central theme of profound social instability highlights an important paradox that has been smouldering since the crisis but surfaces prominently in this year’s report. Global risks transcend borders and spheres of influence and require stakeholders to work together, yet these risks also threaten to undermine the trust and collaboration needed to adapt to the challenges of the new global context.

The world is, however, insufficiently prepared for an increasingly complex risk environment. For the first time, the report provides insights on this at the regional level: social instability features among the three global risks that Europe, Latin America and the Caribbean, and the Middle East and North Africa are least prepared for. Other societal risks, ranging from the failure of urban planning in South Asia to water crises in the Middle East and North Africa, are also prominent. And capacity to tackle persistent unemployment – an important risk connected with social instability – is a major concern in Europe and sub-Saharan Africa.

As in previous years, Part 2 explores three risk constellations that bear on the survey findings. In 2015, these are:

**Interplay between geopolitics and economics:** The interconnections between geopolitics and economics are intensifying because states are making greater use of economic tools, from regional integration and trade treaties to protectionist policies and...
Table 1: The Ten Global Risks in Terms of Likelihood and Impact

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interstate conflict</td>
<td>Water crises</td>
</tr>
<tr>
<td>Extreme weather events</td>
<td>Spread of infectious diseases</td>
</tr>
<tr>
<td>Failure of national governance</td>
<td>Weapons of mass destruction</td>
</tr>
<tr>
<td>State collapse or crisis</td>
<td>Interstate conflict</td>
</tr>
<tr>
<td>Unemployment or underemployment</td>
<td>Failure of climate-change adaptation</td>
</tr>
<tr>
<td>Natural catastrophes</td>
<td>Energy price shock</td>
</tr>
<tr>
<td>Failure of climate-change adaptation</td>
<td>Critical information infrastructure breakdown</td>
</tr>
<tr>
<td>Water crises</td>
<td>Fiscal crises</td>
</tr>
<tr>
<td>Data fraud or theft</td>
<td>Unemployment or underemployment</td>
</tr>
<tr>
<td>Cyber attacks</td>
<td>Biodiversity loss and ecosystem collapse</td>
</tr>
</tbody>
</table>


Urbanization in developing countries: The world is in the middle of a major transition from predominantly rural to urban living, with cities growing most rapidly in Asia and Africa. If managed well, this will help to incubate innovation and drive economic growth. However, our ability to address a range of global risks – including climate change, pandemics, social unrest, cyber threats and infrastructure development – will largely be determined by how well cities are governed.

Governance of emerging technologies: The pace of technological change is faster than ever. Disciplines such as synthetic biology and artificial intelligence are creating new fundamental capabilities, which offer tremendous potential for solving the world’s most pressing problems. At the same time, they present hard-to-foresee risks. Oversight mechanisms need to more effectively balance likely benefits and commercial demands with a deeper consideration of ethical questions and medium to long-term risks – ranging from economic to environmental and societal.

Mitigating, preparing for and building resilience against global risks is long and complex, something often recognized in theory but difficult in practice. Against this backdrop, Part 3 features three proven or promising initiatives that were instituted in response to extreme weather events and climate-change adaptation. The modelling of the Murray-Darling Basin river system in Australia has pioneered innovative methods of water management that are now being adapted for use elsewhere in the world. The Resilient America Roundtable is currently helping selected local communities across the United States to understand how they might be affected by different risks and then design resilience strategies. ZÜRS Public, part of an extensive flood management programme in Germany, is a public-private collaboration that for several years now has been a tool for communicating with homeowners and businesses about their exposure to flood risk.

Over the past 10 years, the Global Risks report has raised awareness of the dangers from the interconnected nature of global risks and has persistently called for multistakeholder collaboration to address them. By offering a broad-ranging overview from risk identification and evaluation to practices – from the “what” to the “how” – this year’s report aims to provide the most comprehensive set of insights yet for decision-makers in its decade-long history.
For the past decade, the Global Risks report – now in its 10th edition – has been calling attention to global risks and providing tools to support decision-makers in their efforts to mitigate or prevent global risks or strengthen resilience against them.

Since its inception, the report has raised awareness that the world is increasingly interconnected and that global risks cannot be seen in isolation. On the contrary, they can have far-reaching cascading effects as demonstrated by the financial crisis in 2008 and its socio-economic consequences. The year 2014 alone witnessed several such risks with potentially broad implications in the years to come if history serves as a benchmark: the frozen relationship between Russia and the West – unfathomable to most just one year ago – seems to be transporting the world back to a time when geopolitics took primacy. The conflict in Syria and the spread of the Islamic State in the region have set off unprecedented migration flows into neighbouring countries and Europe, which could impact social cohesion if poorly managed. Revelations about data fraud and leaks and cyber espionage have critically undermined global trust, running the risk of complicating the search for solutions to other global governance challenges as well.

Successfully addressing these complex and interconnected issues necessitates greater multistakeholder cooperation to increase the capacity to foresee, manage and mitigate global risks and to strengthen society’s preparedness and resilience to them. The report takes the first step towards establishing comprehensive collaboration by fostering a shared understanding of the issues at hand.

10 Years of Risk Awareness Building

Over the past decade, the Global Risks report has seen both its readership and its impact increase significantly. The report has become a useful tool for many governments and businesses to assess their exposure to global risks (see Box 1). It has also successfully raised awareness on key risks, such as the threat of increasing resistance to
antibiotics, which was featured in 2013, or important IT-related risks, which are now at the forefront of business concerns.

After 10 years, the World Economic Forum is now also in a position to revisit the first Global Risks report, an endeavour that illustrates both the difficulty and the necessity of attempting to think 10 years ahead. The economic risk given most attention in 2007 was the possibility of an asset price bubble, which set off a major financial crisis in the same year. The subsequent years were primarily defined by potential risks related to the stability of financial systems in many countries and the threat of sovereign default, resulting in an economic meltdow the world is still recovering from. The interconnected nature of the global economy today and the scale of the global financial crisis show the need to look beyond the obvious for risk interconnections.

Importantly, this 10th edition also reflects a decade of learning and methodological improvements. Fundamentally, the report’s approach remains the same – to identify global risks and their interactions, and to assess them on two dimensions: their perceived likelihood and impact. However, over the years, a number of refinements have been made to the methodology, reflecting the lessons learned from 10 years’ experience in this field. This year’s edition features an updated methodology based on input from the members of the newly established Advisory Board (the list of members appears in the Acknowledgements section at the end of this report).

The uncertainty associated with risks, their interconnected nature and often the absence of data make it difficult to accurately quantify a range of risks – for example social unrest, cyber attacks or oil price shocks. A survey is therefore a suitable tool to get a sense of the order of magnitude of the impact and likelihood of risks. The qualitative, perceptions-based approach embodied in the Global Risks Perception Survey has been the base of the World Economic Forum’s work in this area since 2011, capturing the views of decision-makers from the Forum’s multistakeholder constituencies on the perceived impact and probability of risks and the interconnections between them. Perceptions allow us to better understand decision-makers’ priorities, which in turn influence their decisions.

Over the years, the reports have put increasing emphasis on the interconnected nature of global risks and the potential spillover effects of systemic risks, putting this aspect of risks on the agenda. The resulting complexities underscore the difficulties stakeholders face when addressing risks and are reflected in this edition’s introduction of trends as drivers of risks. As a result, there is increased emphasis on going beyond the analysis of global risks to include suggestions on what stakeholder alliances can do about them. The focus on solutions in this edition is the strongest yet, with a new section on practices and a stronger focus in the survey on preparedness and progress.

### Box 1: How has the Global Risks report been used?

A range of stakeholders were asked how they used the Global Risks report series over the last 10 years. The most common answers were to:

- develop scenarios;
- prepare crisis exercises;
- assess vulnerabilities and their potential for cascade effects;
- inform “sense making” exercises in crisis situations;
- train top decision-makers;
- model risks external to the direct business environment.

Part 1 of this report explores the results of the Global Risks Perception Survey 2014. It explains the distinction between risks and trends, visualizes the likelihood of interconnections between risks, and analyses the difference in risk perceptions over different time horizons. Figures 1, 2 and 3 are shown on the inside cover flaps.

Part 2 deep-dives into three topics that emerged strongly from the interconnections between risks and trends: the interplay between geopolitics and economics, rapid urbanization in developing countries, and emerging technologies.

Part 3 discusses risk management and risk resilience: it presents survey respondents’ views on which risks have most successfully been addressed over the past 10 years, and shares practices from the public and private sectors that offer ways forward to address global risks. The full methodology for the survey is shared in Appendix B. The complete set of data can be explored online at: www.weforum.org/risks.
Introduction

The Global Risks 2015 report comes at a time when various manifestations of global risks brought into sharp relief that the world is not equipped to deal with these events or similar occurrences in the future. For the past decade, the Global Risks report has been calling attention to global risks and providing a base for multistakeholder action. Over this period, the evolution in understanding how global risks are thought about and assessed has been significant. This has led the Forum to update the methodology it has used to assess global risks for the 10th edition of the report, based on input from the members of the newly established Advisory Board.

Building on this evolution, in this report a global risk is defined as an uncertain event or condition that, if it occurs, can cause significant negative impact for several countries or industries within the next 10 years. Based on this refined definition, 28 global risks were identified and grouped into the five customary categories: economic risks, environmental risks, geopolitical risks, societal risks and technological risks. A description of the risks and the methodology employed can be found in Appendix A and Appendix B.

A further development in the 2015 report is the delineation of risks and trends. This distinction allows a better understanding of the underlying drivers of global risks. A trend is defined as a long-term pattern that is currently taking place and that could contribute to amplifying global risks and/or altering the relationship between them. The focus on trends can contribute to risk mitigation; for example, better planned urbanization can help alleviate certain risks that concentrate in urban areas. Moreover, the differentiation between trends and risks emphasizes the fact that trends, unlike risks, are occurring with certainty and can have both positive and negative consequences. Trends are long-term, ongoing processes that can alter the future evolution of risks or the interrelations among them, without necessarily becoming risks themselves.
As in previous years, risks are assessed based on the perception of leaders and decision-makers obtained through the Global Risks Perception Survey. The survey captures the views of the World Economic Forum’s multistakeholder communities across different areas of expertise, geographies and age groups. It was conducted between July and September 2014 and gathered the perceptions of almost 900 leading decision-makers from business, academia and the public sector. A more detailed description of the sample and the survey’s methodology is presented in Appendix B. Complementary to the Global Risks Perception Survey data, the views of business executives were also collected on the risks of highest concern for doing business in their country, presented in more detail in Appendix C.

The results provide a snapshot of current perceptions on global risks and highlight priorities for action from three complementary angles: (1) the Global Risks Landscape, in which risks are assessed according to likelihood and impact, allowing a comparison of how perceptions have evolved over the years (Figure 1); (2) the Interconnections Maps of Risks (Figure 2) and of Risks and Trends (Figure 3); and (3) the level of concern in the short and long terms (Figure 1.1).

The Global Risks Landscape, as defined by the survey, highlights five global risks that stand out as both highly likely and highly potentially impactful (upper right quadrant of Figure 1). Interstate conflict has significantly leaped up both dimensions since 2014, arguably reflecting recent geopolitical conflicts that are fuelling geopolitical and social instability. As last year, concerns about environmental and economic risks remain, in particular around failure of climate-change adaptation, water crises and unemployment and underemployment reflecting concern about how little tangible action has been taken to address them. At the same time, cyber attacks remain among the most likely high-impact risks.

Respondents also underscored the potentially devastating impact of the rapid and massive spread of infectious diseases, which reflects the need for a higher level of preparedness for major pandemics at both the country and international levels to address this important risk (see Box 2.4 in Part 2).

In the geopolitical risks category, respondents identified weapons of mass destruction (WMDs), which include weapons containing nuclear, chemical, biological and radiological technologies, as the third most impactful risk, albeit as the second least likely risk. If deployed, they would create an international crisis with huge human and economic costs. In the coming decades, technological advancements, greater access to scientific knowledge and the increased vulnerability of classified information to cyber threats enhance the risk of WMDs proliferation, particularly in fragile areas. This highlights the need for greater international collaboration to control the proliferation of WMDs.

Among the economic risks, fiscal crises and unemployment are perceived as close to equally impactful and likely as in last year’s report, yet other risk categories take centre stage this year (see Figure 1.4). While the world has made progress in addressing and preventing financial crises, and small improvements in fiscal issues and unemployment have been achieved, the danger of complacency compared to other risks exists: experts remain concerned about significant residual risks, which may have been overshadowed by other risks in the survey.2

The prominence of risks dominating recent headlines in our assessments raises questions about the role of the “availability heuristic” – risks that have manifested themselves recently may be uppermost in people’s minds, even if their recent occurrence does not necessarily increase their impact or likelihood over a 10-year time horizon. To reveal more about the psychology behind the responses, the survey this year asked respondents to nominate risks of highest concern over two time horizons: 10 years, as usual, and 18 months. The results are shown in Figure 1.1. In the short term, respondents are more concerned about global risks related to recent events and human action, including interstate conflict, state collapse, failure of national governance and large-scale terrorist attacks. The list for the longer term is dominated by risks related to physical and environmental trends that have been less prominent in recent headlines, such as water crises, failure of climate-change adaptation and food crises.

Interestingly, the risk of social instability scores high in both the short and long term. This trend towards social fragility is one of five threads that stand out from the 2015 survey – along with growing concern about geopolitics, the possible overshadowing of economic risks by other more imminent risks, concern about unaddressed environmental risks, and persisting vulnerabilities in cyberspace – which are explored in more depth below.
Box 1.1: The evolution of the risks of highest impact/likelihood

As the report’s 10th anniversary approaches, the evolution of the perceived top five global risks can be viewed in terms of impact and likelihood as documented in the Global Risks reports from 2007 to 2015. As Table 1.1.1 shows, economic risks largely dominated from 2007 to 2014, with the risk of an asset-price collapse heading the list in the run-up to the financial crisis, giving way to concerns about the more immediate but slow-burning consequences of constrained fiscal finances, a major systemic financial failure in the immediate post-crisis years, and income disparity. This year features a radical departure from the past decade; for the first time in the report’s history, economic risks feature only marginally in the top five. In the 25th year after the fall of the Berlin Wall, geopolitical risks are back on the agenda. The dispute over Crimea in March 2014 serves as a forceful reminder of the consequences of interstate conflicts with regional consequences that seemed long forgotten and unfathomable, as further explored in this report. Similarly, together with other events in 2014, such as the prominent rise of the Islamic State, it has brought state collapse and the failure of national governance back into public consciousness. At the same time, health-related risks, such as pandemics – last considered impactful in 2008 – have made it back into the unglamorous top, following the unprecedented spread of Ebola.

On a higher level, Table 1.1.1 also indicates a shift over past years away from economic risks in general to environmental risks – ranging from climate change to water crises. While this highlights a recognition of the importance of these slow-burning issues, strikingly little progress has been made to address them in light of their far-reaching and detrimental consequences for this and future generations.

Table 1.1.1: The Evolving Risks Landscape (2007-2015)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>Breakdown of critical information infrastructure</td>
<td>Asset price collapse</td>
<td>Asset price collapse</td>
<td>Asset price collapse</td>
<td>Storms and cyclones</td>
<td>Severe income disparity</td>
<td>Severe income disparity</td>
<td>Income disparity</td>
<td>Interstate conflict with regional consequences</td>
</tr>
<tr>
<td>2nd</td>
<td>Chronic disease in developed countries</td>
<td>Middle East instability</td>
<td>Slowing Chinese economy (-10%)</td>
<td>Slowing Chinese economy (-10%)</td>
<td>Flooding</td>
<td>Chronic fiscal imbalances</td>
<td>Chronic fiscal imbalances</td>
<td>Extreme weather events</td>
<td>Extreme weather events</td>
</tr>
<tr>
<td>3rd</td>
<td>Oil price shock</td>
<td>Failed and faltering states</td>
<td>Chronic disease</td>
<td>Chronic disease</td>
<td>Corruption</td>
<td>Rising greenhouse gas emissions</td>
<td>Rising greenhouse gas emissions</td>
<td>Unemployment and underemployment</td>
<td>Failure of national governance</td>
</tr>
<tr>
<td>4th</td>
<td>China economic hard landing</td>
<td>Oil and gas price spike</td>
<td>Global governance gaps</td>
<td>Fiscal crises</td>
<td>Bodenrvie loss</td>
<td>Cyber attacks</td>
<td>Water supply crises</td>
<td>Climate change</td>
<td>State collapse or crisis</td>
</tr>
<tr>
<td>5th</td>
<td>Asset price collapse</td>
<td>Chronic disease, developed world</td>
<td>Retrenchment from globalization (emerging)</td>
<td>Global governance gaps</td>
<td>Climate change</td>
<td>Water supply crises</td>
<td>Management of population aging</td>
<td>Cyber attacks</td>
<td>High structural unemployment and underemployment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>Asset price collapse</td>
<td>Asset price collapse</td>
<td>Asset price collapse</td>
<td>Fiscal crises</td>
<td>Major systemic financial failure</td>
<td>Major systemic financial failure</td>
<td>Fiscal crises</td>
<td>Water crises</td>
<td></td>
</tr>
<tr>
<td>2nd</td>
<td>Retrenchment from globalization</td>
<td>Retrenchment from globalization (developed)</td>
<td>Retrenchment from globalization (developed)</td>
<td>Climate change</td>
<td>Water supply crises</td>
<td>Water supply crises</td>
<td>Climate change</td>
<td>Rapid and massive spread of infectious diseases</td>
<td></td>
</tr>
<tr>
<td>3rd</td>
<td>Interstate and civil wars</td>
<td>Slowing Chinese economy (-10%)</td>
<td>Oil and gas price spike</td>
<td>Oil price spikes</td>
<td>Geopolitical conflict</td>
<td>Food shortage crises</td>
<td>Chronic fiscal imbalances</td>
<td>Water crises</td>
<td>Weapons of mass destruction</td>
</tr>
<tr>
<td>4th</td>
<td>Pandemics</td>
<td>Oil and gas price spike</td>
<td>Chronic disease</td>
<td>Chronic disease</td>
<td>Asset price collapse</td>
<td>Chronic fiscal imbalances</td>
<td>Diffusion of weapons of mass destruction</td>
<td>Unemployment and underemployment</td>
<td>Intermediate conflict with regional consequences</td>
</tr>
<tr>
<td>5th</td>
<td>Oil price shock</td>
<td>Pandemics</td>
<td>Fiscal crises</td>
<td>Fiscal crises</td>
<td>Fiscal crises</td>
<td>Extreme energy price volatility</td>
<td>Extreme volatility in energy and agriculture prices</td>
<td>Failure of climate change adaptation</td>
<td>Critical information infrastructure breakdown</td>
</tr>
</tbody>
</table>

Note: Global risks may not be strictly comparable across years, as definitions and the set of global risks have evolved with new issues emerging on the 10-year horizon. For example, cyber attacks, income disparity and unemployment entered the set of global risks in 2012. Some global risks were reclassified: water crises and rising income disparity were recategorized as societal risks and as a trend, respectively, in 2015. The 2006 edition of the Global Risks report did not have a risks landscape.
Fragile Societies under Pressure

The fragility of societies is of increasing concern, fuelled by underlying economic, societal and environmental developments (Figure 3 and Figure 1.2). A major driver of social fragility is rising socio-economic inequality within countries, although it is diminishing between countries. Among the members of the Organisation for Economic Co-operation and Development (OECD), the average income of the richest 10% has now grown to about nine times that of the poorest 10%. In other countries, the ratio is even higher: for example, more than 25 times in Mexico.\(^9\)

Income inequality is widening quickly in large emerging markets. The People’s Republic of China has seen its Gini Index rise from about 30 in the 1980s to over 50 in 2010.\(^4\) While extreme poverty (less than $1.25 per day) was reduced from afflicting over 50% of the world’s population in 1990 to 22% in 2010, the same reduction did not take place in those earning under $3 per day.\(^4\) The story is of people escaping extreme poverty, yet remaining poor. Widening income inequality is associated with lower and more fragile economic growth, which reduces the scope to meet rising social expectations in emerging markets.\(^7\)

Rising structural unemployment drives both inequality and social pressures. Lower economic growth and technological change are likely to keep unemployment high in the future, also in developing countries. The spread of connectivity enables protest movements to mount more quickly, increasing the risk of unrest and violence that could easily spill over from individual countries to affect the global economy. While inequality and unemployment contribute to social instability, social instability in turn impacts negatively on equality, employment and wealth creation. The multidirectional cause-and-effect relationship makes it harder to address the related risks.

Underlying social fragility is also the accelerating pace of change, growing complexity and the deepening extent of global interdependence, which together reduce people’s feeling of control over their immediate environment and hence their sense of stability and security. A common psychological response to insecurity and perceived loss of control is the desire to turn inwards towards smaller groups that have a stronger sense of identity. At the same time, increased global connectivity allows people to make their voices heard and to convene with like-minded individuals. The growing risks of social extremism and isolationism are brought to light through the rising influence of religious groups and in the separatist movements in Catalonia and Scotland.

The effects associated with climate change will put further pressure on societies. Its expected impact on the ability to grow food and access water could prompt sudden and uncontrolled population migrations, putting additional pressure on receiving countries.\(^8\) Already in 2014, the number of refugees worldwide from environmental or conflict-related causes reached its highest level since World War II.\(^9\)
Part 2

As societies become less homogenous and less bound by common values, and more polarized into the have and have-nots, they will become harder to govern effectively. This in turn increases the risk of prolonged economic stagnation, creating the potential for a self-reinforcing downward spiral into social chaos. States will need to mitigate this risk through policies to make growth more inclusive: providing social protection, hospitals, schools, public goods and services such as infrastructure.

Growing nationalism is evident around the world: in Russia, as seen in the Crimea crisis; in India, with the rising popularity of nationalist politicians; and in Europe, with the rise of far-right, nationalist and Eurosceptic parties in a number of countries.

Growth and employment creation are currently expected to remain below pre-crisis levels in both emerging markets and advanced economies, suggesting that the drivers of nationalism will remain strong, and raising the possibility of more frequent and impactful conflicts among states. Importantly, as can be seen in Figure 2, interstate conflict is no longer physical but uses economic means and cyber warfare to attack people’s privacy as well as intangible assets.

Geopolitical risks can have cascading impacts on other risks. As state structures are challenged by conflict, the risk of the failure of national governance and state collapse or crisis can increase in areas where current state boundaries do not necessarily reflect popular self-identification. A recent example is Iraq and Syria, where ISIS has claimed control of territory and attracted 20,000 to 30,000 fighters from a near standing start.10 The rapid rise and brutality of ISIS as well as the response of the international community may underlie the increased likelihood and impact attributed by respondents to the risk of the deployment of weapons of mass destruction and the higher potential impact than in previous years associated with large-scale terrorist attacks (Figure 1.3).

Failure of national governance features strongly this year, as the third most likely risk across the global risks landscape. This risk area captures a number of important elements around the inability to efficiently govern as a result of corruption, illicit trade, organized crime, the presence of impunity and generally weak rule of law. Over past years, the links between many forms of global crime and corruption and their impact on global security, extremism, terrorism and fragile states have only grown stronger, and it is critical to acknowledge and address them through more effective policies that curb illegal financial flows, foster transparent governance and build capacity around anti-crime efforts at the national and local levels. Absent a stronger response from both the public and private sectors, the risk is of undoing hard-won gains in economic and political stability, and further eroding trust in leadership. In a number of countries, such as India, Indonesia and Romania, new leaders have been elected in large part due to their public commitment to more transparent and corruption-free governance models, underscoring an ongoing shift in public expectations.

The growing interconnectedness of the global economy increases the economic effects of any geopolitical conflict. Supply chains that run across countries in conflict could be interrupted, leading to disruptions in the availability of goods or energy. Survey respondents considered the risk of an energy price shock to the global economy as more impactful and more likely than in previous years, despite the increasing availability of shale gas or alternative energy sources. The interplay between economic and geopolitical forces is further explored in Part 2 of this report.
Box 1.2: The rising threat from non-state actors

The group known as ISIS, ISIL or the Islamic State has gained global notoriety through its taste for video-recorded executions and large-scale atrocity, with a background of further human rights abuse that includes arbitrary imprisonment and sexual enslavement. While its thirst for violence, blood and misery – and especially the way it glories in these crimes – mark it out from other non-state armed forces of our age, this is really only a quantitative distinction. Other groups – many of them part of the global Al Qaeda franchise – do the same, only less. Al Nusra in Syria, Al Qaeda in the Islamic Maghreb and the Nigerian group known in the West as Boko Haram all do some of what ISIS does on a somewhat smaller scale.

But what really marks ISIS out is that it has claimed statehood and with that has established some of the machinery of state management. ISIS has not only proclaimed the new Caliphate, the rule of the successors of the Prophet Muhammad – not that it has any theological credibility to do so – but also administers the area of northern Iraq and eastern Syria where it holds sway. It handles law and order, some social services on a selective basis, and has an intelligence service and system of informers set up for it by former officials of the overthrown Ba’athist regime of Saddam Hussein. Adding to the lavish funds it has raised from the Gulf region, it has also taken over and emptied the central bank in Mosul, making it the richest non-state armed force in the world and equipping it to be a non-state state.

The phenomenon is not without precedent: the Provisional Revolutionary Government in South Vietnam did much the same in the late 1960s and early 1970s, without the self-glorification of atrocity and terror. And it is not without parallel today. The Taliban have effective control over parts of Afghanistan and was effectively the state in the late 1990s, until the US-led offensive overthrew it in October 2001. Among other examples, for a long time FARC has been in control of large areas of Colombia, while the Seleka militia is in charge of northern areas of Central African Republic. Having withdrawn from Bangui in January 2014 under heavy international pressure, they are recuperating by systematically taxing gold and diamond mining, livestock and other economic activities – behaving in part like a nascent state. Some groups have not based themselves outside the territory over which they are fighting, but have waged warfare that is not territorially limited. In the Al Qaeda mode, they have fought what they perceive to be a global enemy. Today, perhaps the trend is in the opposite direction: re-entry into an era of the non-state state.
Economic Risks: Out of the Spotlight?

The global economy is returning to growth, albeit sluggishly, and there is a feeling that significant progress has been made in reducing the likelihood of another financial crisis (as explored in Box 1.4). This may reflect a false sense of control, as history shows that people do not always learn from past failures and are often taken by surprise by the same risks.

The global unemployment rate is expected to remain at current levels until 2018, reflecting a growing problem of structural unemployment in advanced economies. This will likely keep wages low, maintaining deflationary pressures; in the Eurozone, inflation fell as low as 0.66% in 2014. As past years have seen a build-up of debt in many major economies – notably China, where the corporate debt-to-GDP ratio went from 92% in 2003-2007 to 110% in 2013 – the possible risk is that deflation could reduce debtors’ ability to repay, threatening the future stability of the financial system.

Conversely, low interest rates have also fuelled the risk of asset bubbles. Since the financial crisis, the use of expansionary monetary policy – such as quantitative easing and zero interest rates – has not had the expected impact of significantly increasing credit availability in the real economy, instead leading to a reflation of asset prices. Credit booms and asset bubbles have historically resulted in bank bailouts and recession in the real economy (see Box 1.3).

The risks of a failure of a major financial mechanism or institution and fiscal crises are perceived as equally impactful and likely as in last year’s report (Figure 1.4), yet other risks, such as water crises, interstate conflict and the failure of climate-change adaptation, have taken centre stage. This runs the risk of diverting decision-makers’ attention away from continuing economic reforms. Despite recent efforts (see Box 1.4), either deflationary pressures or the bursting of an asset-price bubble could still cause the failure of a major financial mechanism or institution – especially as the shadow banking sector is less regulated yet increasingly important. Likewise, in many countries public debt levels are still worryingly high so that the related risks are likely to persist over many years.

Decision-makers’ focus on other risks could lead to inaction at a time when continued progress in structural reform is most necessary; The Global Competitiveness Report 2014-2015 outlines some priorities. Maintaining the momentum of both financial and fiscal reforms will be crucial to avoid another major economic crisis.

If macro-prudential regulation fails again, central banks will be left with only one tool – monetary policy – to pursue both goals of economic and financial stability. This may prove impossible. Trying to prick bubbles by using monetary policy risks causing a bond market rout and a hard landing for the real economy. Keeping monetary policy loose in a bid to help the real economy risks inflating asset bubbles that will, inevitably, eventually burst and also damage the real economy. Loose monetary policy is the mother of all bubbles. Attempting to walk this tightrope will be a difficult issue for central banks in both advanced and emerging markets in the years to come.

Box 1.3: Asset bubbles – a new old risk?

The evidence of frothiness is increasing in a number of housing markets in both advanced and emerging economies – including Canada, the United Kingdom, Switzerland, France, Sweden, Norway, China, Hong Kong SAR and Singapore – as well as in a number of credit and equity markets across the world.

The traditional goal of central banks has been economic stability: keeping inflation low while achieving robust growth. The current realization is that central banks must also seek to preserve financial stability – which means, among other things, avoiding risky bubbles. The current theory is that macro-prudential regulation and supervision of the financial system will avoid bubbles and achieve financial stability. However, bubbles are very hard to identify (price increases could also reflect market movements), and macro-prudential regulation has not historically been effective and excludes the unregulated shadow banking system.
Box 1.4: Recent advances in the global regulation of the financial system

The global financial system is undergoing massive structural change as a result not only of the crisis but of the regulatory changes in its wake. The very fact that the whole post-crisis regulatory overhaul has been spearheaded by the Financial Stability Board and G20, i.e. with explicit political backing by a global set of policy-makers, is very innovative and has not been the case in setting international regulatory standards before. The past five years have witnessed a profound change of international regulatory standards for banks and non-banks alike.

♦ Banks’ regulatory rules have been revised (usually subsumed under the Basel III heading), resulting in stronger capital requirements, the first-ever globally agreed liquidity standards (for a short-term liquidity and a structural funding measure), and new standards for constraining large exposures and improving risk management. Also, supervisory standards are being raised and the international standard setter (Basel Committee) has launched a programme to assess national implementation, which exerts peer pressure on jurisdictions to implement the reforms in a consistent manner.

♦ Cross-border resolution difficulties witnessed in the crisis are reflected in the new set of expectations with regard to effective resolution regimes and a process of recovery and resolution planning for the largest banks, complete with setting up cross-border crisis management groups composed of authorities from the (most prominent) jurisdictions where these banks operate.

♦ Regarding non-banks, the international community is finalizing a basic solvency requirement for global insurers who are systemically important – to date there has been no global solvency standard; over-the-counter derivatives markets are undergoing major overhaul with measures aimed at mandating and/or incentivizing central clearing and trading on organized platforms with reporting to trade repositories of all contracts. In terms of insurance regulation, many countries in Europe, Latin America and Asia are adopting variants of the Solvency II regime. New insurance regulation has a strong emphasis on corporate governance, disclosure and accountability. These measures are relevant as they aim to change the broader corporate behaviour.

♦ International accounting standards are being changed, in particular to make loss recognition more forward-looking (newly issued IFRS9).

♦ Some supervisory authority over the financial sector has been relocated to central banks, most notably in Europe, where the European Central Bank has taken on additional responsibilities.

Still, of course, challenges remain. Addressing the issue of “too-big-to-fail” remains a key issue. Efforts are needed to: (i) finalize living wills and identify and remove barriers to firms’ resolvability; (ii) reach consensus on banks’ loss-absorbing capacity to ensure that they can be resolved; (iii) address obstacles to cross-border cooperation and recognition of resolution measures; (iv) ensure recovery and resolution of non-banks; and (v) promote better regulation of the shadow banking sector. Cross-border challenges persist also in over-the-counter derivatives reform. As regulatory regimes developed in parallel in the two largest markets (European Union and United States), they resulted in a framework that overlaps and is not completely consistent. Regulatory decisions allowing reliance on home regulatory regimes (known as “deference”) are urgently needed. Trade reporting requirements have been adopted in key countries but legal barriers frustrate implementation. Progress on trading standardized contracts on exchanges and electronic trading platforms continues to slip. Political commitment is needed to advance reforms in all these areas.

Source: This box draws on the latest Global Financial Stability Report and related IMF work.
Note: In addition to the current regulatory reforms described above, some experts believe that profound changes in the corporate culture and incentive systems in the financial sector are needed to reduce excessive risk-taking.
**Box 1.5: Black Sky – risks to critical infrastructure**

The world has more to lose than ever before from massive failure of critical infrastructure. To improve efficiency and lower cost, various systems have been allowed to become hyperdependent on one another. The failure of one weak link – whether from natural disaster, human error or terrorism – can create ripple effects across multiple systems and over wide geographical areas.

Large-scale power outages might be the most visible illustration. The initiating event in the August 2003 power failures in the United States occurred in Ohio but the worst consequences were felt by 55 million people in the north-eastern part of the United States and Canada. The July 2012 India blackout was the largest in history, affecting 670 million people, about 10% of the world population, and was partially triggered by high demand during a heat wave.

In many countries, infrastructure has not been maintained well enough to withstand the kinds of catastrophes that could spark such cascading effects. This is often the result of procrastination, the perception that the risk is so small that it is not worth considering or crowding out by other priorities, and the fact that investing in preparedness is rarely immediately rewarded in the electoral process. The challenge is financial, and incentives are misaligned. For example, in the United States, over 80% of infrastructure is owned or managed by private sector firms, which are not responsible for the negative externalities that failure of their part of the infrastructure could have elsewhere. 1 To increase investment in infrastructure, a coordinated, global, long-term and multistakeholder approach is required. Upgrading infrastructure is essential, in recognition that resilient infrastructure has become the backbone of a competitive economy.

---

**Environment – High Concern, Little Progress**

Over the past decade, awareness has grown regarding the threats posed by environmental change to social, political and economic security. As the Global Risks Perception Survey 2014 highlights, three of the top 10 risks in terms of impact over the next 10 years are environmental risks: water crises, at the top of the table, and failure of climate-change adaptation as well as biodiversity loss (see Figure 1).

**Figure 1.5: The Changing Global Risks Landscape 2014-2015, Environmental Risks**

Both water crises and failure of climate-change adaptation are also perceived as more likely and impactful than average (upper right quadrant of Figure 1 and Figure 1.5). Global water requirements are projected to be pushed beyond sustainable water supplies by 40% by 2030. 16 Agriculture already accounts for on average 70% of total water consumption and, according to the World Bank, food production will need to increase by 50% by 2030 as the population grows and dietary habits change. 15 18 The International Energy Agency further projects water consumption to meet the needs of energy generation and production to increase by 85% by 2035. 19

---

Note:

1 Auerswald, Branscomb, LaPorte and Michel-Kerjan, 2006.
The Intergovernmental Panel on Climate Change notes that weather extremes in food-producing regions are already causing price increases and suggests that the impact of climate change on weather patterns and rainfall – causing either floods or droughts – could cut crop yields by up to 25%.20

The nexus of food, water, energy and climate change has been identified by the US National Intelligence Council as one of four overarching mega trends that will shape the world in 2030.21 The risks interconnections map (see Figure 2) shows how survey respondents perceived this nexus to be related also to other risks, including large-scale involuntary migration.

Decision-makers will be forced to make tough choices about allocations of water that will impact users across the economy (Part 3 of this report highlights an approach developed in Australia’s Murray-Darling Basin, for addressing this issue). The situation will worsen further if more man-made environmental catastrophes causing shocks to the system happen: more recent examples include the Fukushima power plant disaster threatening to contaminate both freshwater and seawater, or the Deepwater Horizon oil spill contaminating large sections of coast along the Gulf of Mexico.

Overfishing, deforestation and the inadequate management of sensitive ecosystems such as coral reefs are increasing the stress on food and water systems. Major biodiversity loss and ecosystem collapse was assessed as high impact by respondents, but below average in terms of likelihood (see Figure 1); the latter seems to reflect a misperception. The World Bank estimates that 75% of the world’s poor, or 870 million people, make a living from ecosystems, including tourism and the goods they produce, while 350 million are affected by the loss of coral reefs.22 Increasingly, decision-makers are realizing that biodiversity loss is not a second-order issue but is intricately linked to economic development, food challenges and water security.

The urgency of coordinated global action on climate change was reinforced in April and November 2014 by the Intergovernmental Panel on Climate Change’s release of its Fifth Assessment Report and the associated update. It reconfirms that warming is unequivocally happening and it is “extremely likely” that human influence has been the dominant cause. Atmospheric concentrations of three major greenhouse gases (carbon dioxide, methane and nitrous oxide) are at their highest level in 800,000 years. Strong evidence of the effects of climate change is already apparent, in terms of sea level rise, shrinking glaciers, warmer oceans and the increasing frequency of weather extremes.

Even though all of these risks are well known, governments and businesses often remain woefully underprepared, as illustrated by respondents’ perceptions that relatively little progress has been made on these risks in the last decade (see Figure 3.1). At the heart of the problem is a risk-management approach based on responsive measures that assume things go back to normal after a crisis – an approach that falls short with complex or slowly evolving environmental risks such as climate change. Stakeholders have been slow to address the underlying causes of environmental risks or to address their economic, social, political and humanitarian consequences.

Box 1.6: The road to Paris – is 2015 make or break for climate change?

In 2015 the international community has a once-in-a-generation opportunity to align the climate change and development agenda. A series of global summits on climate change, disaster risk reduction, financing for development and sustainable development goals could embed into the post-2015 global governance architecture a coherent agenda for tackling interlocking environmental risks.

Convergence among governments on these decisions could kick-start the next generation of sustainable growth and poverty reduction – through catalysing private finance and scaling low-carbon, climate-resilient investment, especially but not only in developing countries. However, the opportunity will be missed if governments continue to value narrow short-term concerns above the prospect of longer-term global prosperity and environmental security. More vulnerable populations will be consigned to the negative spiral of poverty and environmental degradation.

Until recently, the expectation was that governments would struggle to finalize a strong global climate accord in time for the Paris climate conference in December 2015. But is the tide beginning to turn? At the United Nations Secretary-General’s Climate Summit in September 2014, over 1,000 businesses and investors signalled their support for global carbon pricing. So did some 73 countries, covering 52% of global GDP and 54% of global emissions.

Major consumer companies and financial institutions see the need to reduce global climate risks and have mobilized action along their supply chains, for example through the New York Declaration on Forests and the move towards climate-friendly coolants. The Oil & Gas Climate Initiative signalled refreshed engagement from major energy producers.

The hope is that these coalitions of committed businesses could both inject concrete solutions and create a more positive global atmosphere for governments to collectively make decisions in 2015. A positive signal is the agreement between China and the United States in November 2014. A strong set of clear policy signals to the wider business community is needed from the world’s governments on their ambition to tackle environmental risks. The year 2015 is not an opportunity the world can afford to miss.
Technological Risks: Back to the Future

The risk of large-scale cyber attacks continues to be considered above average on both dimensions of impact and likelihood (see Figures 1 and 1.6) This reflects both the growing sophistication of cyber attacks and the rise of hyperconnectivity, with a growing number of physical objects connected to the Internet and more and more sensitive personal data – including about health and finances – being stored by companies in the cloud. In the United States alone, cyber crime already costs an estimated $100 billion each year.23

Figure 1.6: The Changing Global Risks Landscape 2014-2015, Technological Risks

The IoT is likely to disrupt business models and ecosystems across a range of industries. While this will deliver innovation, the prospect of many large players across multiple industries being forced to change so radically at the same time raises potential systemic risks such as large-scale disruption in labour markets and volatility in financial markets. A major public security failure could also prevent the IoT from becoming truly widespread.

An important characteristic of global risks, which transpires across the cases included in this report, is their interconnectedness, shown in the Interconnections Map in Figure 2. It is important to stress that risks cannot be seen in isolation. The feedback loops between risks and the fact that they are also driven by underlying trends (Figure 3) raise their complexity and make it more difficult to control individual risks. Over past years, the speed of transmission and the strength of interconnections have increased.

The complexity of addressing risks, their likelihood and their potential consequences raise the question of preparedness, on the global, regional, national and local levels.

Box 1.7: Governing the Internet — the need for mechanisms to maintain a unified and resilient network

The pace of innovation and the highly distributed nature of the Internet require a new approach to global Internet governance and cooperation. As more people rely on the Internet, the question of Internet governance becomes increasingly important. Two kinds of issues exist: technical matters, to make sure all the infrastructure and devices that constitute the Internet can talk to each other; and overarching matters, to address cyber crime, Net neutrality, privacy and freedom of expression.

Responsibility for the technical infrastructure of the Internet is dispersed among several organizations, including the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C), the Regional Internet Registries (RIRs), the root servers’ operators, and the Internet Corporation for Assigned Names and Numbers (ICANN). The solutions they propose – policy models, standards, specifications or best practices – spread through voluntary adoption or ad hoc conventions, regulations, directives, contracts or other agreements.

No such systems exist for developing and implementing solutions to the overarching issues. Consequently, governments are feeling pressure to enact national measures to deal with their citizens’ data and privacy concerns. While laws that force the “localization” of infrastructure may be easier short-term solutions than collaborating to define global mechanisms for addressing the issues, the risk is that “data nationalism” could endanger the network effects that underlie the Internet’s ability to drive innovation and create social and economic value.

To advance the conversation, identify possible solutions and contribute to open, resilient and inclusive Internet governance, the World Economic Forum is embarking on a multiyear strategic initiative to bring together leaders from the public and private sectors with civil society leaders and the technical community to address these issues in an impartial, high-level dialogue. This effort will complement the expert-level discussions taking place at the Internet Governance Forum and various other grassroots and government-led initiatives.


**Preparedness at the Regional Level Is Different**

As most efforts to address global risks are undertaken at the national and regional levels, it is important to look at preparedness from a disaggregated perspective. Figure 1.7 illustrates for each world region those risks for which survey respondents indicated their region is the least prepared. Preparedness reflects a combination of exposure to a risk and the measures that have already been taken to mitigate or prepare for it.

It is striking that every region presents a wholly different set of issues for which it is least prepared. For example:

- **High structural unemployment or underemployment** is seen as the risk for which **Europe** is least prepared, followed by large-scale involuntary migration and profound social instability. Both unemployment and migration flows into Europe are expected to remain high on the agenda going forward and are driving factors of social instability.24

- **North America** identifies failure/shortfall of critical infrastructure, large-scale cyber attacks and failure of climate-change adaptation as the three risks for which it is least prepared. Major breakdowns of infrastructure in the wake of Superstorm Sandy and the sheer number of cyber attacks illustrate the low level of preparedness.

- **Sub-Saharan Africa** is considered least prepared for infectious diseases and unemployment. Both are of key importance given recent events and the fact that strong population growth is expected to exacerbate unemployment in the coming years, despite expected economic growth.

- **Many regions**, including Europe, Latin America and the Caribbean, and the Middle East and North Africa, also include profound social instability among the risks they are least prepared for.

- **East Asia and the Pacific** is perceived as least prepared for interstate conflict and failure of urban planning. It is also the only region that reported being least prepared for man-made environmental catastrophes following the 2011 Fukushima incidence.

- Failure of urban planning is among the first three risks in East Asia and the Pacific, **Latin America and the Caribbean**, and **South Asia**. In such regions, urbanization is especially rapid and the failure of urban planning can lead to a wide range of catastrophic scenarios from social unrest to pandemic outbreak (Part 2).

---

**Figure 1.7: For Which Global Risks Is Your Region Least Prepared?**


Note: Respondents were asked to select three global risks that they believe their region is least prepared for. For legibility reasons, the names of the global risks are abbreviated. Please see Appendix A for the full name and description. Oceania is not displayed because of the low number of respondents.
Conclusion

Drawing on the perceptions of almost 900 survey respondents, this chapter focuses on the threats of social fragility and short-term worries about conflict. Rising socio-economic inequality, weak economic growth, food price volatility and food insecurity, unemployment, large-scale migration and the growing heterogeneity and interdependence of societies are among the key drivers of social fragility. Growing social polarization, isolationism and nationalism in turn have the potential to trigger geopolitical conflicts.

The section highlights the interconnections between global risks and trends. A better understanding of global risks and the interconnections between them is key to prompting discussion about how to prepare, mitigate and prevent them. Part 2 of this report analyses in detail selected clusters of interconnected risks and how they could evolve – the interplay between geopolitical and economic risks, challenges related to urbanization in developing countries and emerging technologies.

Endnotes

1 The risk of water crises is classified as a societal risk for the purpose of this report. However, it has an important environmental dimension.
3 OECD, 2011.
4 Standardized World Income Inequality Database. See http://myweb.uiowa.edu/fsolt/swiid/swiid.html.
5 The Gini index measures the extent to which the distribution of income among individuals or households within an economy deviates from a perfectly equal distribution on a scale from 0 (perfect equality) to 100 (perfect inequality).
6 UN, 2014.
9 UNHCR, 2014.
12 IMF, 2014b.
13 IMF, 2014c.
15 As mentioned above, the risk of water crises is classified as a societal risk for the purpose of this report. However, it has an important environmental dimension.
20 Porter et al., 2014.
21 NIC, 2012.
24 In the first nine months of 2014, the number of migrants crossing the Mediterranean Sea into Europe reached 160,000, twice the previous record from 2011. Integrating such a large number of migrants is a big challenge, which has the potential to destabilize societies if not properly addressed.
25 Global risks may not be strictly comparable across years, as the names and description of the risks were revised between 2014 and 2015. The risks introduced in 2015 are not displayed in the figures and only the risks for which the name or the description were slightly revised between 2014 and 2015 are presented. Water crises was categorized as an environmental risk in 2014 but as a societal risk in 2015. To ensure legibility, the names of the global risks are abbreviated. Please see Appendix A for the full name and description.
References


Part 2: Risks in Focus

2.1 Introduction

This section of the Global Risks 2015 report presents deep-dives into three “risks in focus” – the interplay between geopolitics and economics, rapid and unplanned urbanization in developing countries, and emerging technologies – that emerged from the Risks Interconnections Map and the Risks-Trends Interconnections Map (see Figures 2 and 3). These provide good illustrations of the links between different global risks. The analysis in the following pages is based on follow-up research and interviews with experts.

As discussed in Part 1, geopolitical risks are back, as evident from the central node of the failure of national governance in the interconnections maps, and the strong linkages to interstate conflict and profound social instability, among others. With economies tied together on an unprecedented scale by financial and trade flows, many analysts are concerned about the resurgence of the trend towards the interplay between geopolitics and economics. While national governments in the past also made use of economic tools to increase their relative power, today’s strong economic ties arguably make this interplay more complex and therefore more difficult to navigate. This resurgence could have profound implications for the effectiveness of global governance mechanisms in other areas, from combating climate change to reaching an international solution for Internet governance.

Even as nation states step up their efforts to maintain or expand power, urbanization is slowly but surely rebalancing the locus of power from national to city governments. The data gathered for this report suggest that urbanization is a critical driver of profound social instability, failure of critical infrastructure, water crises, and the spread of infectious diseases (see Figure 3). This will only be further exacerbated by an unprecedented transition from rural to urban areas: by 2050, two-thirds of the world’s population – an estimated 6.3 billion people – will live in cities, with 80% in less developed regions. Rapid and unplanned urbanization in these regions has the potential to drive many risks. How effectively the world addresses global risks, ranging from climate
change to pandemics, will increasingly be determined by how well cities are governed. The concentration of a large number of people, assets, critical infrastructure and economic activities means that the risks materializing at the city level have the potential to disrupt society.

From artificial intelligence to synthetic biology, the need for governance on a global scale comes into focus when considering emerging technologies, given the many uncertainties about how emerging technologies evolve and their far-reaching economic, societal and environmental implications. The data also point to strong interconnections with man-made and natural environmental catastrophes (see Figure 2). The coming years are likely to see rapid advances in such fields as artificial intelligence and synthetic biology – and while many of their impacts are likely to be beneficial, negative effects will spread quickly in today’s hyperconnected world. Some of those negative effects may be difficult to anticipate and safeguard against.

In many cases, by addressing the trends underlying most of the risks, the vulnerability to risks can be reduced significantly. In addition, understanding the context and possible trajectories of a significant nexus of risks and trends can help to clarify ways to address them and to capitalize on opportunities presented by the trends. That is the aim of the analysis that follows.

2.2 Global Risks Arising from the Accelerated Interplay between Geopolitics and Economics

Geopolitics traditionally focuses on military might, resources and demographics as measures of national influence, while economics focuses on growth, productivity and prosperity. However, geopolitics and economics have been intertwined through history – for example in the rise of British political power on the back of the "economic" Industrial Revolution, the era of British and French colonialism, or the Cold War, when a deep geopolitical divide separated economies. When the Cold War ended, an era of common norms ushered in a global economy; now, more than 25 years after the fall of the Berlin Wall, strategic competition is returning. The world is grappling with a seemingly accelerating dynamic between geopolitics and economics. Today’s realpolitik is not ideologically driven, includes new players and takes place in the context of deep economic integration.

Will the global economy, the efficiency of the international system and the win-win logic of commerce be undermined by geopolitics? How will economic decisions and spheres of influence impact the global balance of power? What global risks could emerge when countries use economic rather than military tools to advance their ends? These questions have been brought into focus by trends including the recent heightened tensions in East Asia, the acceleration of regional integration in South-East Asia and the rise of preferential and regional trade agreements more generally, the shale gas and oil revolution in the United States, turbulence in the Middle East and Ukraine, competing integration mechanisms in Latin America, China’s assertion of leadership in the global economy, and acts of terrorism and violent strife that are redrawing borders and sending economies backwards.

Global interconnectedness and the rising speed of information transmission have reinforced the interdependence between geopolitics and economics, with cyberspace representing an important new front in the geopolitical equation as cyber attacks have the growing potential to inflict economic damage. This makes it difficult for decision-makers to predict the development of such situations as sanctions and other instruments of economic coercion, thus raising the risk of unintended consequences. The interplay between geopolitics and economics can create, reinforce and alter the nature of the interconnections between global risks, affecting many areas of public policy and international cooperation.

Governments and businesses alike need to conduct “geopolitical due diligence” to not be caught off guard. The focus below is on three areas where direct effects are likely – disruptions to international trade, and threats to political cooperation and the international rules-based system.

How Is this Situation Manifested?

In a retreat from the prevailing logic of globalization that characterized the 1990s and early 2000s, today’s international environment is in large part marked by self-interested nation states trying to gain relative power over others, even at the expense of economic considerations. Rising unemployment and more difficult fiscal situations are contributing to the more inward orientation of economies. The growth of trade along global value chains and intensifying financial linkages have increased the economic cost of rising protectionist policies, such as tariffs, sanctions and trade wars, as described in Box 2.1.

As states turn inwards, their international economic policies tend to focus on collaboration with smaller groups of like-minded countries that would allow them to better pursue their economic goals. Countries have always sought to achieve both geopolitical and economic aims through regional economic integration – the European Economic Community, for example, was established to stabilize relations and raise the stakes in case of war as well as to increase market size and economic opportunities. Many regional groupings are established as they allow countries to gain relative power over others. This type of thinking is currently why the Association of Southeast Asian Nations (ASEAN) is seeking to create a unified market by
Table 2.1: East Asian-Pacific Free Trade Agreements

<table>
<thead>
<tr>
<th>Country</th>
<th>RCEP¹</th>
<th>TPP²</th>
<th>FTAAP³</th>
<th>Korea, Rep. bilateral⁴</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Brunei</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Cambodia</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>China, People’s Rep.</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Indonesia</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Japan</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Korea, Rep.</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Malaysia</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>New Zealand</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Philippines</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Singapore</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Thailand</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>Vietnam</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
</tbody>
</table>

- 🟢 Part of the agreement
- 🟢 Not part of the agreement

Source: ASEAN, Ministry of Foreign Affairs of the Republic of Korea, The Economist and Oliver Wyman analysis.

Notes: ¹ RCEP, promoted by ASEAN, would also include Cambodia, India, Laos and Myanmar.
² TPP, promoted by the US, would also include Canada, Chile, Mexico and Peru as well as the US.
³ FTAAP, promoted by China, would also include Hong Kong SAR, Papua New Guinea, Russian Fed. and Taiwan, China.
⁴ Planned or achieved. Korea’s free trade agreements (additionally with Brunei, Cambodia, Indonesia, Malaysia, Philippines, Singapore, Thailand and Vietnam) are through its agreement with ASEAN.

2015 and pursuing an agreement on a Regional Comprehensive Economic Partnership (RCEP). It is also one of the drivers of the United States’ efforts to pursue discussions on two major free trade and investment agreements – the Transatlantic Trade and Investment Partnership (TTIP) and the Trans-Pacific Partnership (TPP).

However, in some cases competing integration agreements are creating strategic competition: in Latin America, the Pacific Alliance and Mercosur provide different models of integration; in Ukraine, the country was torn between the European Union and the Eurasian Economic Union; and Asian countries need to assess the US-led TPP and the ASEAN-led RCEP. As illustrated by Table 2.1, the current situation is a complex mix of overlapping and competing regional negotiations.

A driver of the intensifying interplay between economics and geopolitics is the growing direct role of the state in the world economy, which is affecting traditional trade and investment flows and potentially enabling countries to exert geopolitical influence through economic dependency. This trend is manifested in increasing state-led investments in other countries’ infrastructure, such as in the case of Chinese investment in Africa or Latin America; strategic investments by sovereign wealth funds and state-owned enterprises in land and businesses in other countries, as seen in the case of Gulf economies’ investments in Africa, and government purchases of other governments’ debt. In August 2014, China and Japan held 7.2% and 7% of US debt, respectively.

To strengthen their geopolitical position, countries have also reverted to measures that control access to economically important national resources or the prices of commodities over which they exert monopoly power to undermine other economies’ performance. These potential ways to leverage power over other countries through economic links are increasingly becoming an explicit part of foreign policy thinking.

In today’s interdependent global economy, whenever countries focus on their domestic market – even if the decisions are taken by central banks rather than politicians – there is potential for unintended effects on other countries to spill over into the geopolitical sphere. For instance, one side effect of Japan’s expansionary monetary policies to restart its domestic...
the year before, as reported in August
reduced by 26.1% in comparison to
Germany’s exports to Russia were
supply chains. One effect is
review the architecture of their
restricted access to specific sets of
the Russian Federation have
imposed by the European Union and
European countries, while sanctions
disruptions in the supply of gas to
Federation. The latter has caused
between Ukraine and the Russian
the Middle East and the dispute
outbreak in West Africa, tensions in
supply chains include the Ebola
smooth functioning of global
Recent specific examples of threats
to the smooth functioning of global
supply chains include the Ebola
outbreak in West Africa, tensions in
the Middle East and the dispute
between Ukraine and the Russian
Federation. The latter has caused
disruptions in the supply of gas to
European countries, while sanctions
imposed by the European Union and
the Russian Federation have
restricted access to specific sets of
goods and forced some companies
to review the architecture of their
supply chains. One effect is
Germany’s exports to Russia were
reduced by 26.1% in comparison to
the year before, as reported in August
2014.

economy has been the devaluation of
the yen by about 50% in recent years,
much to the detriment of its neighbours,
while quantitative easing in the United
States has impacted international
capital flows into emerging markets.

Global Risks Emerging from
the Interplay between
Geopolitics and Economics

Opinion polls show that the public in
countries such as Japan, Germany
and the United States are increasingly
ea sceptical about the benefits of trade
and foreign investment, even as their
governments push for increased
liberalization. Despite progress on the
trade facilitation agreement, the larger
Doha Round of trade negotiations has
stalled, costing an estimated $180
billion per year at the global level.
Negotiations of regional agreements
are also being questioned (one example
is TTIP in Germany). Although growing
again, global flows of foreign direct
investment remain down by more than
a quarter from their 2007 peak, and
international trade growth has slowed
since 2012. It has yet to be determined,
however, whether this is merely a
cyclical or structural phenomenon
heralding a phase of de-globalization
in which globalized markets give way
to regional groupings and to a rise in
protectionist measures.2

When confronted with political and
economic volatility at home, countries
often revert to protectionism under the
guise of policies to reduce risk. A recent
OECD report shows that despite their
professed commitment to free trade,
G20 economies have increasingly
reverted to protective measures since
growth slowed in 2012 in the wake of
the global financial crisis.3 Protectionism
can take different forms. It can be
related, for example, to the protection
of strategic sectors, local content
requirements in the case of external
investment, or state bailouts.

Economic sanctions are another type
of punitive geo-economic measure,
such as the tit-for-tat engaged in by
Russia and the West, which indicates
that some countries are ready to
countenance a long period of economic
hardship and diplomatic woe to achieve
their political goals. The risk is thus
significant that if the use of punitive
geo-economic measures becomes
more widespread, a growing number of
countries may revert to protecting
national producers and supply chains,
which could considerably impact global
trade flows. The economic effects of
sanctions can include slow growth,
unemployment and fiscal pressures.
Taken together, the slowdown in
globalization, the rise in protectionism
and the increasing prevalence of
sanctions could give rise to a scenario
of slower growth in advanced and
emerging economies. Slower growth
in emerging economies could translate
into social unrest and political instability
if the aspirations of large portions of the
population cannot be met.

The Increasing Risk to the
Architecture of Global Governance

Much of the interplay between
economic and geopolitical interests
plays out not in the trade arena but
in the Bretton Woods institutions.
Countries’ inability to agree on an
institutionalized, closer coordination
of macroeconomic policies to reduce
global imbalances provides an
interesting example. Some observers
see the failure to mitigate these
imbalance, combined with the return
of strategic competition in an era
defined by an erosion of trust, as raising
tail-risk possibility of undermining the
Bretton Woods institutions themselves
and the international rule-based system
more generally.

These developments are reflected in
the recent alternative structures being
established by selected countries.
Brazil, Russia, India and China in 2014
set up the New Development Bank,
the so-called BRICs Bank, which
is intended to lend up to $34 billion
globally, particularly for infrastructure
projects. In the same year, together
with 20 other countries, China created
the Asian Infrastructure Investment
Bank for the Asia-Pacific region. Much
as a retreat from global multilateralism
is worrisome, stronger regional
multilateralism is not necessarily a bad
ting, as regional solutions to regional
problems can be consistent with global
governance structures. As already
noted, although economic integration
is not often explicitly targeted, it binds
nations more closely together politically.
Some observers see the current push

Box 2.1: Global supply chains – too lean?

With the opening of markets
worldwide and the reduction of
barriers to the flow of goods and
capital, the creation of value has
become a complex process
spanning countries and continents.
The far-reaching global supply chains
set up by multinational corporations
are more efficient, but the complexity
and fragility of their interlinkages
make them vulnerable to systemic
risks, causing major disruptions.
These comprise natural disasters,
including those related to climate
change; global or regional
pandemics; geopolitical instability,
such as conflicts, disruptions of
critical sea lines of communication
and other trade routes; terrorism;
large-scale failures in logistics;
unstable energy prices and supply;
and surges in protectionism leading
to export/import restrictions.

Recent specific examples of threats
to the smooth functioning of global
supply chains include the Ebola
crisis in West Africa, tensions in
the Middle East and the dispute
between Ukraine and the Russian
Federation. The latter has caused
disruptions in the supply of gas to
European countries, while sanctions
imposed by the European Union and
the Russian Federation have
restricted access to specific sets of
goods and forced some companies
to review the architecture of their
supply chains. One effect is
Germany’s exports to Russia were
reduced by 26.1% in comparison to
the year before, as reported in August
2014.
for RCEP as a means to restore trust in Asia, stabilize security situations and find solutions at a regional level to other ongoing problems.

Some observers also see the TPP and TTIP as the last chance for the United States and Europe to bring many developing countries into alignment with a liberal economic institutional framework by creating a domestic market big enough to be able to set the rules in the global economy – an implicit recognition that current global governance institutions are no longer functioning effectively enough to achieve this goal. Yet, increasingly, negotiating countries question the benefits of these mega regional agreements.

Any weakening of global governance could weaken collective resilience to global risks, which respect no national borders and require multilateral responses. These include climate change, where an inability to agree on carbon reductions could result in rising sea levels, more frequent storms and stress to water supplies; migration flows, where pressures on societies and resources could result in conflict; and Internet governance, where a tendency towards fragmentation can already be observed through some large economies’ efforts to put into place measures to protect their national networks. Should a global governance solution to the Internet not be found further fragmentation could significantly reduce the benefits of communication and information networks that the world has come to take for granted.

**What Can Be Done?**

At a time of highly interconnected challenges that can only be addressed through global cooperation, reducing the barriers to international collaboration is crucial, as no collaboration is the worst possible outcome. What can stakeholders do to strengthen international collaboration and to reduce the risk of negative effects of geo-economic measures?

Many of the challenges related to international collaboration reflect a lack of trust among the key players. Strengthening trust among leaders and populations in global economies is therefore key to ensuring effective collaboration at a time when strategic competition dominates international relations. Without trust, no decisions at the international level will be taken. However, the responsibility extends beyond the political level: multinational companies and consumers also have a role to play to strengthen the argument in favour of global collaboration in the face of growing pressures to prioritize national economic self-interest.

**Conclusion**

Faced with competing strategic pivots and governments’ growing tendency to look inwards and prioritize their domestic producers and economies, and with an increased reliance on economic levers as a means to gain geopolitical influence, the coming years could see competitive relationships between the major powers develop into trade and currency wars, requiring economic diplomacy.

While regional institutions and alternative structures have a role, global institutions must respond to pressure to better reflect the rising wealth and power of emerging economies. They remain the most promising means for competing powers to build strategic trust, which could minimize the detrimental effects of geo-economic competition on growth and prosperity.

---

**Box 2.2: The World Economic Forum’s work on geo-economics**

The World Economic Forum is developing a clearer understanding of the interaction between geopolitics and economics with the support of its Network of Global Agenda Councils. The Global Agenda Council on Geo-economics aims to become the world’s leading network of thinkers on the impact of geopolitics on the global economy and vice versa – launching a vital global discussion that links leaders from the worlds of politics, economics and business in a debate about the major trends that are changing the world. The Council will publish an annual brief identifying the main geo-economic issues on the horizon and delve into the implications of emerging developments, such as the use of sanctions or low oil prices for different regions, actors and sectors. Issues that will be examined in more depth include the next phase of economic warfare, the next wave of state capitalism (including the rise of central banks as drivers of geo-economics and the rise of strategic sectors), the idea of gate globalization, the role of infrastructure in building alliances, and the weakening of peripheral countries by regional agreements. The Forum’s work will also include an assessment of impact on selected industries. It will be developed over the coming years and the findings will be integrated into the work of the Forum and its communities.
2.3 City Limits: The Risks of Rapid and Unplanned Urbanization in Developing Countries

The world is experiencing a historically unprecedented transition from predominantly rural to urban living. In 1950, one-third of the world’s population lived in cities; today the number has already reached more than one-half, and in 2050 city dwellers are expected to account for more than two-thirds of the world’s population (see Figure 2.1). This rapid rise will mainly take place in developing countries (see Figure 2.2). Africa and Asia – both still comparatively less urbanized than other regions – will be the fastest urbanizing regions with the urban population projected to reach 56% in Africa and 64% in Asia by 2050 (currently at 40% and 48%, respectively). These developments imply an unprecedented shift of the urban world away from the north-west to the south and east.

If managed well, urbanization can bring important benefits for development. Cities are an efficient way of organizing people’s lives: they enable economies of scale and network effects, and reduce the need for transportation, thereby making economic activity more environmentally friendly. The proximity and diversity of people can spark innovation and create employment as exchanging ideas breeds new ideas. The diversity of cities can also inculcate social tolerance and provide opportunities for civic engagement. Already today, the linkages between cities form the backbone of global trade, and cities overall generate a large majority of the world’s GDP.

One of the main factors driving rapid urbanization in emerging economies is rural-urban migration motivated by the prospect of greater employment opportunities and the hope of a better life in cities. Indeed, when a certain critical mass of population is reached, it is economically viable to deliver many infrastructure projects, such as public transportation. However, a higher population density also creates negative externalities, especially when urbanization is rapid, poorly-planned and occurs in a context of widespread poverty. Estimates suggest that 40% of the world’s urban expansion is taking place in slums, exacerbating socio-economic disparities and creating unsanitary conditions that facilitate the spread of disease. The example of the 1994 outbreak of pneumonic plague in the Indian city of Surat suggests how, in a worst-case scenario, poverty and a pandemic in a large-scale informal settlement could potentially lead to a breakdown in urban order.

Rapid urbanization can alter the nature of almost every global risk considered in this report by influencing its likelihood and impact. In addition, cities are points of convergence of many risks, which make them particularly vulnerable to chain reactions and amplify the interconnection between global risks. Better knowledge of how such risks interconnect in their materialization at the city level is the first step towards helping cities build resilience. Three regions – South Asia, East Asia and the Pacific, and Latin America and the Caribbean – have identified this risk as among those for which they are the least prepared (Figure 1.7 and for more details see: www.weforum.org/risks). The following sections consider four selected and particularly daunting urban challenges: infrastructure, health, climate change and social instability.

Figure 2.1: Global Urban Population Growth (1950-2050)

Figure 2.2: Forecasted Urban Population Growth 2010-2050


The Infrastructure Challenge

The quality of a city’s infrastructure – its housing, electricity, roads, airports, public transport, drinking water, sanitation, waste management, flood defences, telecommunications, hospitals, schools and so forth – largely determines its residents’ quality of life, social inclusion and economic opportunities. It also largely determines the city’s resilience to a number of global risks, in particular environmental, social and health-related risks, but also economic risks, such as unemployment. Indeed, the availability and quality of infrastructure are at the core of many of the challenges faced by rapidly urbanizing cities in developing countries, which are developed further in this section of the report.

As cities in developing countries are expanding rapidly, it is likely that infrastructure will not be able to keep pace with their growth nor the increased expectations of their populations. Action to close the infrastructure gap is urgently needed and will strongly influence the potential of risks to have catastrophic cascading effects.

To provide adequate global infrastructure for electricity, road and rail transport, the OECD estimates that telecommunications and water will cost approximately $71 trillion by 2030 – an enormous challenge as it represents about 3.5% of forecasted global GDP. Most of this investment will be needed in emerging economies. For instance, Development in Africa estimates that approximately $71 trillion by 2030 – an enormous challenge as it represents about 3.5% of forecasted global GDP. Most of this investment will be needed in emerging economies. For instance, Development in Africa estimates that $48 billion per year to be financed. Consequently, cities are looking for public-private collaboration to involve the private sector in the design, construction and maintenance of infrastructure. However, to promote successful public-private collaboration, corruption must be tackled, as it is a traditional problem in construction projects and dissuades investors. In addition, the key enablers of public-private collaboration at the city level include factors such as transparency (in such matters as partner selection and contract execution) and the availability of accurate data to allow risk assessments. Public-private collaboration is a way for cities to

Box 2.3: Life in the city – how smart is smart?

Like industry, cities are increasingly investing in information technology-based systems to address the challenges of managing large enterprises and enabling service innovations. While these investments often deliver rapid improvements in efficiency and operational continuity, they also create unexpected new risks: bugs and brittleness.

The growing amount of software used to manage urban infrastructure increases the likelihood of coding errors that can cause catastrophic failures, especially in highly-centralized control systems. For instance, in 2006, San Francisco’s Bay Area Rapid Transit network was laid low for days when initial efforts to fix a bug inadvertently triggered a larger and longer outage.

Smart city systems also rely on many underlying technology platforms that are surprisingly brittle. For example, the Global Positioning System (GPS) is not only electrical power and “backhaul” connections to the communications grid can fail: both the Japanese tsunami in 2011 and Superstorm Sandy in 2012 caused damage to cellular networks that took weeks to repair. The most dangerous failure mode for cellular networks is due to congestion – during crises, panic dialling frequently overwhelms the carefully-managed wireless spectrum these networks depend on.

The brittleness of mobile cellular networks presents a special challenge to resilience for large cities. Unlike the Internet – which, at least in theory, possesses significant resilience through its multiple, redundant linkages – cellular networks have several choke points. Cell sites themselves can be damaged physically. More importantly, the supporting wired infrastructures for electrical power and “backhaul” connections to the communications grid can fail: both the Japanese tsunami in 2011 and Superstorm Sandy in 2012 caused damage to cellular networks that took weeks to repair. The most dangerous failure mode for cellular networks is due to congestion – during crises, panic dialling frequently overwhelms the carefully-managed wireless spectrum these networks depend on.

All levels of government will need to be more assertive in auditing and stress-testing vital digital infrastructures. The sudden and unexpected failure of these systems during crises has crippling knock-on effects across official and civilian response and relief efforts. Even during peacetime, the economic and social effects of bugs and brittleness can be devastating, with potential for long-lasting impacts. Assessments must go beyond cybersecurity, as the risks are not just about external threats but also about the fundamentally unstable dynamics of digital infrastructures and the complex, chaotic and unpredictable ways they can interact with civic, social and economic systems.

Where will the money come from? Most governments are under tight budget constraints and many developing countries already spend a large proportion of their national income to meet the basic needs of their population. Consequently, cities are looking for public-private collaboration to involve the private sector in the design, construction and maintenance of infrastructure. However, to promote successful public-private collaboration, corruption must be tackled, as it is a traditional problem in construction projects and dissuades investors. In addition, the key enablers of public-private collaboration at the city level include factors such as transparency (in such matters as partner selection and contract execution) and the availability of accurate data to allow risk assessments. Public-private collaboration is a way for cities to

The Infrastructure Challenge

The quality of a city’s infrastructure – its housing, electricity, roads, airports, public transport, drinking water, sanitation, waste management, flood defences, telecommunications, hospitals, schools and so forth – largely determines its residents’ quality of life, social inclusion and economic opportunities. It also largely determines the city’s resilience to a number of global risks, in particular environmental, social and health-related risks, but also economic risks, such as unemployment. Indeed, the availability and quality of infrastructure are at the core of many of the challenges faced by rapidly urbanizing cities in developing countries, which are developed further in this section of the report.

As cities in developing countries are expanding rapidly, it is likely that infrastructure will not be able to keep pace with their growth nor the increased expectations of their populations. Action to close the infrastructure gap is urgently needed and will strongly influence the potential of risks to have catastrophic cascading effects.

To provide adequate global infrastructure for electricity, road and rail transport, the OECD estimates that telecommunications and water will cost approximately $71 trillion by 2030 – an enormous challenge as it represents about 3.5% of forecasted global GDP. Most of this investment will be needed in emerging economies. For instance, Development in Africa estimates that approximately $71 trillion by 2030 – an enormous challenge as it represents about 3.5% of forecasted global GDP. Most of this investment will be needed in emerging economies. For instance, Development in Africa estimates that approximately $71 trillion by 2030 – an enormous challenge as it represents about 3.5% of forecasted global GDP. Most of this investment will be needed in emerging economies. For instance, Development in Africa estimates that approximately $71 trillion by 2030 – an enormous challenge as it represents about 3.5% of forecasted global GDP.
identify where cooperation can address problems that neither municipalities nor the private sector can solve alone (for example in advanced telecommunications infrastructure) and both will have a major role to play.

Much discussion revolves around the potential for technology to increase the efficiency with which urban infrastructure can be managed. The use of big data, the Internet of Things and ubiquitous smartphones promise to revolutionize aspects of city management, from keeping traffic flowing to reducing electricity outages, tackling crime and preparing for emergencies. Developing countries have the opportunity to leapfrog by avoiding the mistakes made by more advanced countries and applying the lessons learned from the development of smart city infrastructure. However, while “smart cities” should work better, they may also be more vulnerable to cyber error or terror (see Box 2.3). When discussing “smart cities” it is important to note the human component. Indeed, if technology developed for smart cities does not embrace universal design to ensure use by all (including the disabled and the elderly), its benefits could be controversial.

Cities and Health

In most countries, the health of city dwellers has improved through better access to education and healthcare, better living conditions and targeted public-health interventions. However, the vulnerability of urban centres to pandemics points to the need for strong public-private coordination involving organizations beyond the traditional healthcare sector. The ability to mobilize a response from sectors as diverse as food production, telecommunications and corporate supply chains will determine how epidemics are fought in the future. Local, national and cross-border government agencies need to build bridges with all stakeholders and learn from what worked in the past to shape systems with the capacity to respond to pandemics and build the resilience to bounce back afterwards. Coordinating responses and developing global governance mechanisms are critical to contain future outbreaks, which will inevitably occur.

Box 2.4: Health in cities – robust plans are needed to face the threat of pandemics

Dense urban living facilitates the spread of infectious diseases. Particular vulnerabilities exist in countries where rapid urbanization results in informal settlements that make it difficult to control transmission and can therefore increase the risks of mosquito-transmitted epidemics, such as malaria, tuberculosis, dengue and yellow fever.

Various examples highlight the impact of urbanization on pandemics. In the Democratic Republic of the Congo, 83% of people with tuberculosis live in cities (around 40% of the population lives in urban areas). In 2009, Mexico City shut down schools, libraries, museums and nightclubs to halt the spread of H1N1 flu. A 2009 cholera epidemic in Zimbabwe heavily affected Harare city, Chitungwiza and Kadoma, also stressing the influence of slums and the lack of urban infrastructure as key igniting factors for the speed and severity of disease outbreaks.

In today’s hyperconnected world, it is easier for pathogens to be carried from one city to another and quickly scale up the impact of most outbreaks. The presumed introduction of the virus to the informal settlements of Kenema and Freetown in Sierra Leone has undoubtedly augmented its spread. Sierra Leone is urbanizing at a rate of 3% each year, and in 2005 more than 97% of its urban population lived in slums. The economic impact of Ebola is enormous for the affected countries and their neighbouring countries. The estimated economic cost is $32 billion in the worst-case scenario.

Another aggravating factor to the 2014 Ebola crisis was the lack of a governance mechanism that would allow an effective link between what was being observed at the country and city levels and the alert mechanisms necessary to trigger an emergency response. Looking into the future for an adequate response across geographies, the existence of such a governance mechanism would: (i) allow collaboration between local and national governments, civil society and the private sector across borders; (ii) coordinate the surveillance, collection, sharing and analysis of infectious disease data in real time; (iii) incentivize the private sector to develop and scale up the production and distribution of affordable drugs, vaccines and diagnostics; (iv) establish a network of centres for research into microbial threats; and (v) promote international standards for best laboratory, regulatory and ethical practice.

The vulnerability of urban centres to pandemics points to the need for strong public-private coordination involving organizations beyond the traditional healthcare sector. The ability to mobilize a response from sectors as diverse as food production, telecommunications and corporate supply chains will determine how epidemics are fought in the future. Local, national and cross-border government agencies need to build bridges with all stakeholders and learn from what worked in the past to shape systems with the capacity to respond to pandemics and build the resilience to bounce back afterwards. Coordinating responses and developing global governance mechanisms are critical to contain future outbreaks, which will inevitably occur.

Notes:
4 Gire et al., 2014.
6 Rubin and Saidel, 2014.
One excellent case study is the city of Surat in India. Hitting rock bottom due to a public health disaster in 1994, it introduced measures to drastically raise hygienic standards, making it one of the cleanest cities in India today.10 However, when urbanization is rapid and unplanned, a combination of high population density, poverty and lack of infrastructure – especially water and waste management – can create the conditions for communicable diseases to flourish.

Almost 700 million urban dwellers currently lack adequate sanitation.17 The problem is particularly acute in Sub-Saharan Africa and south-central Asia, where 62% and 43%, respectively, of the urban population live in slums.18 Such conditions create increased risks of illnesses, worm infections, cholera and diarrhoea – a leading cause of preventable death in children – and help spread emerging infectious diseases, such as Severe Acute Respiratory Syndrome (SARS) and H1N1 influenza.19 With the projected huge increase of populations living in slums and the growing sophistication of transport networks between cities, the spread of infectious diseases could happen extremely quickly and could be difficult to contain, creating the risk of global disease outbreaks.

In addition to communicable diseases, rapid and unplanned urbanization is a key driver in the increased prevalence of non-communicable diseases (NCDs) and their key risk factors, such as unhealthy diets, physical inactivity, tobacco consumption, harmful use of alcohol and pollution.20 NCDs, including cardiovascular diseases, diabetes, cancer and chronic respiratory diseases, are the leading cause of death globally. These diseases affect high-, middle- and low-income countries. Every year 38 million people die from NCDs; over 14 million die prematurely – before they reach the age of 70 and 85% are in low- and middle-income countries.21

The prevalence of diabetes in emerging economies is rising: in China, it is already comparable to that in the United States: in 2013, the figures were 9% and 9.2%, respectively. In Kuwait, diabetes prevalence has been as high as 23%; even in a low-income country such as Burundi, it reached 4.5%.22 Although a formal link between diabetes and urbanization has not been established, the number of urban dwellers with diabetes in low- and middle-income countries is projected to almost double from 181 million today to 347 million people in 2035.23 In India for example, diabetes prevalence is close to epidemic proportion and is attributed - at least partially - to urbanization.24 This will put huge pressure on already fragile healthcare systems, the collapse of which could have devastating cascading effects with dramatic economic losses.

Addressing non-communicable diseases will require efforts to tackle the causes of air pollution, which is estimated to have caused 7 million deaths in 2012.25 Air pollution tends to be more of a problem in developing than developed countries, in part due to coal-fired power plants and the use of biomass for cooking and heating, but mostly due to private transport vehicles.26 Over 90% of air pollution in developing world cities is attributed to old, poorly-maintained vehicles running on low-quality fuel and to roads prone to traffic jams.27 The rapid rise of non-communicable diseases in low-income countries could jeopardize poverty reduction and limit inclusive outcomes from growth.

**Cities and Climate Change**

In many developing countries, migration from rural areas to cities is at least partially driven by the increasing prevalence of extreme weather, such as land degradation and desertification, making agriculture more difficult. For example, many people are migrating from dry land areas in north-east Brazil to favelas in Rio de Janeiro.28 The rapid, inadequate and poorly planned expansion of cities in developing countries can also leave urban populations highly exposed to the effects of climate change. For example, cities tend to be located near the sea or natural waterways, where they are more at risk of flooding. Indeed, 15 of the world’s 20 megacities – those with over 10 million inhabitants – are located in coastal zones threatened by sea-level rise and storm surges.29

The concentration of people, assets, critical infrastructure and economic activities in cities exacerbates the potential of natural catastrophes to cause unprecedented damage: heatwaves, extreme rainfall and drought-related shortages of water and food will increasingly test the resilience of infrastructure in these and other cities. The effects of shortfalls are likely to be felt mostly by the poor, whose informal settlements tend to be on land at especially high risk from extreme weather.30 Making cities more resilient to extreme weather events should be a priority for both local governments and the private sector.

Cities not only need to adapt to climate change, they also have a major role to play in mitigating its impact. While established cities with efficient mass transit systems have relatively low carbon footprints, the early phases of urbanization tend to generate massive greenhouse gas emissions as the construction of infrastructure uses concrete and metals that are carbon-intensive to manufacture.31 Developing countries already account for around two-thirds of annual greenhouse gas emissions, caused in part by their economic growth and rapid urbanization.32 The rapid expansion of their cities means that mitigation measures have to be taken today to help tackle climate change.

With adequate land-use planning and in coordination with the private sector, cities can develop infrastructure in more sustainable, low-carbon ways – but this requires governance, technical, financial and institutional capacities that are often lacking in developing countries.33 Leadership within local governments is at the heart of both urban mitigation of and adaptation to climate change.34 Well-governed cities with universal provision of infrastructure and services have a strong base for building resilience to climate change if processes of planning, design and allocation of human capital and material resources are responsive to emerging climate risks.

**Social Instability**

Cities’ capacity to generate prosperity already largely determines global growth; just over half the world’s
population lives in cities, but they generate more than 80% of global GDP. In addition, most future growth will be generated by midsized cities and not by megacities, as is commonly believed. Ultimately, new migrants in cities are expected to create greater economic value than they would have in the countryside. However, even when cities are successful, the process of absorbing migrants into urban economies is not necessarily smooth. While moving to a city offers individuals more opportunities to improve their living conditions, the high cost of living and competition for livelihoods can also trap people in poverty.

Many of the risks described above can lead to social instability. It is the rapid and unplanned nature of urbanization, rather than urbanization itself, that is linked by many researchers to such risks as urban violence and social unrest. Rapid urbanization in the developing world can quickly bring together large numbers of unemployed youth, a common ingredient of social unrest. Widening inequalities also tend to be more starkly visible in urban than rural areas, with the most wealthy areas of cities often neighbouring quickly-expanding slums. The combination of inequality, competition over scarce resources such as land, impunity from the law and weak city governance increases the risk of violence and potential breakdowns in law and order. Some cities in developing countries are already extremely dangerous, such as for example San Pedro Sula in Honduras, with 169 killings per 100,000 residents in 2011.

Rapid urbanization and the related growing demand for housing are creating pressure on the housing market and social tensions are expected to increase. The shortage of affordable housing not only contributes to social exclusion, it can also threaten to destabilize the wider economy if the housing price increase fuels property bubbles. Making housing more accessible, affordable and adequate for urban dwellers is therefore of critical importance. A wide portfolio of policies, from limiting excessive credit to optimizing land use and development activity in cities, is crucial to mitigate these risks and equitably distribute the benefits of urban growth.

Conclusion: The Importance of City Governance

Urbanization creates opportunities but also exacerbates risks, and the speed at which it is happening challenges our capacity to plan and adapt. This is particularly true in developing economies. For rapid urbanization to provide opportunities to all, carefully considered urban planning and good governance with effective regulatory frameworks are required. However, governments of rapidly-growing cities often have little time for adjustment and learning. As a consequence, inadequate planning and ineffective governance can bring significant economic, social and environmental costs, threatening the sustainability of urban development.

The inability of governments to provide appropriate infrastructure and public services is at the core of many urban challenges in developing countries, which range from the incapacity to contain infectious disease to the challenges of building climate-resilient cities. At the same time, these challenges have worsened due to the rapid and chaotic development of cities. City leaders from government, civil society and the private sector are ideally positioned to plan rapid urbanization and must act to sustain metropolitan growth.

What is more, as the world continues to urbanize, power will increasingly be concentrated in cities. This power – ranging from economic to social – not only makes cities the centre of gravity, but offers greater scope to find practical solutions to the most pressing challenges. Indeed, many observers and organizations are now focusing on cities and the connections between them rather than directing their attention at the national level. The strength of city-level institutions in addition to national institutions – their capacity to be flexible, innovative and dynamic, and effectively involve multiple stakeholders in governance – will largely determine whether urbanization makes the world more resilient or more vulnerable in the face of global risks.
2.4 Engineering the Future: How Can the Risks and Rewards of Emerging Technologies Be Balanced?

From networked medical devices to the Internet of Things, from drought-resistant crops to bionic prosthetics, emerging technologies promise to revolutionize a wide range of sectors and transform traditional relationships. Their impacts will range from the economic to the societal, cultural, environmental and geopolitical.

Emerging technologies hold great and unprecedented opportunities. Some examples are explored in detail in three boxes presented in this section:

♦ Synthetic biology could create bacteria that turn biomass into diesel (Box 2.6).
♦ Gene drives could assist in the eradication of insect-borne diseases such as malaria (Box 2.7).
♦ Artificial intelligence is behind advances from self-driving cars to personal care robots (Box 2.8).

Discoveries are proceeding quickly in the laboratory, and once technologies demonstrate their usefulness in the real world, they attract significantly more investments and develop at an even greater pace.

However, how emerging technologies evolve is highly uncertain. Their potential second- or third-order effects cannot easily be anticipated, such that designing safeguards against them is difficult. Even if the ramifications of technologies could be foreseen as they emerge, the trade-offs would still need to be considered. Would the large-scale use of fossil fuels for industrial development have proceeded had it been clear in advance that it would lift many out of poverty but introduce the legacy of climate change? Would the Haber-Bosch process have been sanctioned had it been evident it would dramatically increase agricultural food production but adversely impact biodiversity? A range of currently emerging technologies could have similar or even more profound implications for mankind’s future. Survey respondents highlighted technological risks as highly connected to man-made environmental catastrophes.

Emerging technology is a broad and loose term (see Box 2.5), and debate about potential risks and benefits is more vigorous in some areas than in others. In the examples that follow, the focus is on technologies that are considered to have wide benefits and for which there is strong pressure for development, as well as high levels of concern about potential risks and safeguards.

Causes for Concern

Risks of undesirable impacts of emerging technologies can be divided into two categories: the foreseen and the unforeseen. Some examples of foreseen risks are leakage of dangerous substances through difficulties of containment (as is sometimes the case with trials of genetically-modified crops) or storage errors (as with 2014 security failures in US disease-control labs handling lethal viruses); the theft or illegal sale of emerging technologies; computer viruses, hacker attacks or human transplants, or chemical or biological warfare. The establishment of new fundamental capabilities, as is happening for example with synthetic biology and artificial intelligence, is especially associated with risks that cannot be fully assessed in the laboratory. Once the genie is out of the bottle, the possibility exists of undesirable applications or effects that could not be anticipated at the time of invention. Some of these risks could be existential—that is, endangering the future of human life (see Boxes 2.6 to 2.8).

Both foreseen and unforeseen risks are amplified by the accelerating speed and complexity of technological development. Exponential growth in computing power implies the potential for a tipping point that could significantly amplify risks, while hyperconnectivity allows new ideas and capabilities to be distributed more quickly around the world. The growing complexity of new technologies, combined with a lack of scientific knowledge about their future evolution and often a lack of transparency, makes them harder for both individuals and regulatory bodies to understand.

Box 2.5: Classifying emerging technologies

In general, three broad categories of emerging technologies can be distinguished: first, those to do with information, the Internet and data transfer, which include artificial intelligence, the Internet of Things and big data; second, biological technologies, such as the genetic engineering of drought-resistant crops and biofuel, lab-grown meat, and new therapeutic techniques based on RNA, genomics and microbiomes; and third, chemical technologies, those involved in making stronger materials (such as nanostructure carbon-fibre composites) and better batteries (through germanium nanowires, for example), recycling nuclear waste and mining metals from the by-products of water desalination plants.

However, any attempt to categorize emerging technologies is difficult because many new advances are interdisciplinary in nature. In particular, information technology underlies many, if not all, advances in emerging technology. A final category of cross-over technologies would include smart grids in the electricity supply industry, brain-computer interfaces and bioinformatics—the growing capacity to use technology to model and understand biology.

Note:
1 RNA stands for ribonucleic acid; it is one of the three major biological macromolecules that are essential for all known forms of life (along with DNA and proteins). A central tenet of molecular biology states that the flow of genetic information in a cell goes from DNA through RNA to proteins: “DNA makes RNA makes protein”. Proteins are the workhorses of the cell: they play leading roles in the cell as enzymes, as structural components, and in cell signalling, to name just a few. For more information see the RNA Society at http://www.rnasociety.org/about/what-is-rna/.
Box 2.6: Synthetic biology - protecting mother nature

For thousands of years, humans have been selectively breeding crops and animals. With the discovery of DNA hybridization in the early 1970s, it became possible to genetically modify existing organisms. Synthetic biology goes further: it refers to the creation of entirely new living organisms from standardized building blocks of DNA. The technology has been in development since the early 2000s, as knowledge and methods for reading, editing and designing genetics have improved, costs of DNA sequencing and synthesis have decreased, and computer modelling of proposed designs has become more sophisticated. (see Figure 2.6.1)

In 2010 Craig Venter and his team demonstrated that a simple bacterium could be run on entirely artificially-made DNA. Applications of synthetic biology that are currently being developed include producing biofuel from E. coli bacteria; designer organisms that act as sensors for pollutants or explosives; optogenetics, in which nerve cells are made light-sensitive and neural signals are controlled using lasers, potentially revolutionizing the treatment of neurological disorders; 3D-printed viruses that can attack cancer; and gene drives as a possible solution to insect-borne diseases (as discussed in Box 2.7).

Alongside these vast potential benefits are a range of risks. Yeast has already been used to make morphine; it is not hard to imagine that synthetic biology may allow entirely new pathways for producing illicit drugs. The invention of cheap, synthetic alternatives to high-value agricultural exports such as vetiver could suddenly destabilize vulnerable economies by removing a source of income on which farmers rely. As technology to read DNA becomes more affordable and widely available, privacy concerns are raised by the possibility that someone stealing a strand of hair or other genetic material could glean medically-sensitive information or determine paternity.

The risk that most concerns analysts, however, is the possibility of a synthetized organism causing harm in nature, whether by error or terror. Living organisms are self-replicating and can be robust and invasive. The terror possibility is especially pertinent because synthetic biology is “small tech” – it does not require large, expensive facilities or easily-tracked resources. Much of its power comes from sharing information and, once a sequence has been published online, it is nearly impossible to stop it: a “DIYbio” or “biohacker” community exists, sharing inventions in synthetic biology, while the International Genetically Engineered Machines competition is a large international student competition in designing organisms, with a commitment to open-sourcing the biological inventions.

Conceivably, a single rogue individual might one day be able to devise a weapon of mass destruction – a virus as deadly as Ebola and as contagious as flu. What mechanisms could safeguard against such a possibility? Synthetic biology and affordable DNA-sequencing also opens up the possibility of designing bespoke viruses as murder weapons: imagine a virus that spreads by causing flu-like symptoms and is programmed to cause fatal brain damage if it encounters a particular stretch of DNA found only in one individual.

Figure 2.6.1: Number of Entities Conducting Research in Synthetic Biology

![Figure 2.6.1: Number of Entities Conducting Research in Synthetic Biology](image)

Source: The Wilson Center 2013
Notes: The “Other” category consists of “Community lab space”, “Military lab” and “Hybrid research/policy”.
No data are available for the categories “Community Lab Space”, “Military Lab”, and “Hybrid Research Institution/Policy Center” in 2009 and for the region Asia/Oceania in 2009
Synthetic biology is currently governed largely as just another form of genetic engineering. Regulations tend to assume large institutional stakeholders such as industries and universities, not small and medium-sized enterprises or amateurs. The governance gap is illustrated by the controversy surrounding the very successful 2013 crowdsourceing of bioluminescent plants, which exploited a legal loophole dependent on the method used to insert genes. The Glowing Plants project, which aims ultimately to make trees function as street lights, was able to promise to distribute 600,000 seeds without any oversight by a regulatory body other than the discretion of Kickstarter. The project caused concern not only among activists against genetically-modified organisms, but also among synthetic biology enthusiasts who feared it might cause a backlash against the technology.

Differences can already be observed in the focus of DIYbio groups in Europe and the United States due to the differing nature of regulations on genetically-modified organisms in their regions, with European enthusiasts focusing more on “bio-art.” The amateur synthetic biology community is very aware of safety issues and pursuing bottom-up options for self-regulation in various ways, such as developing voluntary codes of practice. However, self-regulation has been criticized as inadequate, including by a coalition of civil society groups campaigning for strong oversight mechanisms. Such mechanisms would need to account for the cross-border nature of the technology, and inherent uncertainty over its future direction.

Notes:
2 See 3dprint.com article “Autodesk Genetic Engineer is Able to 3D Print Viruses, Soon to Attack Cancer Cells”; http://3dprint.com/19594/3d-printed-virus-fights-cancer/.
4 See Inter Press Service News Agency article “Synthetic Biology Could Open a Whole New Can of Worms”; http://www.ipnews.net/2014/10/synthetic-biology-could-open-a-whole-new-can-of-worms/.
8 See NCBI literature “European do-it-yourself (DIY) biology: Beyond the hope, hype and horror”; http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4158858/.
10 See “The Principles for the Oversight of Synthetic Biology”; http://www.biosafety-info.net/file_dir/151489162746071c0e12ea.pdf.
11 Zhang, J.Y. et al., 2011.

Safeguards and Challenges

As illustrated by the boxes on synthetic biology, gene drives and artificial intelligence, governance regimes that could mitigate the risks associated with the abuse of emerging technologies – from formal regulations through private codes of practice to cultural norms – present a fundamental challenge that has the following main aspects. The current regulatory framework is insufficient. Regulations are comprehensive in some specific areas of emerging technology, while weak or non-existent in others, even if conceptually the areas are similar. Consider the example of two kinds of self-flying aeroplane: the use of autopilot on commercial aeroplanes has long been tightly regulated, whereas no satisfactory national and international policies have yet been defined for the use of drones.

Spatial issues include where to regulate, whether at the national or international level. The latter is further complicated by the need to translate regulations into rules that can be implemented nationally to be fully enforceable. Undesirable consequences have the scope to cross borders, but cultural attitudes differ widely. For example, public attitudes are more accepting of genetically-modified produce in the United States than the European Union; consequently the EU has institutionalized the precautionary principle, while there is more faith in the US that a “technological fix” will be available for most challenges. Safeguards, regulations and governance need to combine consistency across countries with the strength to address the worldwide impacts of potential risks and the flexibility to deal with different cultural preferences.

The timing issue is that decisions need to be taken today for technologies that have a highly uncertain future path, the consequences of which will be visible only in the long term. Regulate too heavily at an early stage and a technology may thus fail to develop; adopt a laissez-faire approach for too long, and rapid developments may have irrevocable consequences. Different kinds of regulatory oversight may be needed at different stages: when the scientific research is being conducted, when the technology is being developed, and when the technology is being applied. At the same time, the natural tendency to think short term in policy-making needs to be overcome. Compared with Internet technology, notably the physical and life sciences have longer cycles of development and need governance regimes to take a long-term approach. History shows that it can take a long time to reach international agreements on emerging threats – 60 years for bioweapons, 80 years for chemical weapons – so it is never too early to start discussions.

The question of who regulates becomes significant when it is unclear where a new device fits into the allocation of responsibility across existing regulatory bodies. This is an increasingly difficult
Box 2.7: Gene drives – promises and regulatory challenges

In sexually reproducing organisms, most genes have a 50% chance of being inherited by offspring. However, natural selection has in some cases favoured certain genes that are inherited more often. For the past decade or so, research has been exploring how this could be triggered. The “gene drives” method “drives” a gene through a population, stimulating a gene to be preferentially inherited. This gene then can spread through a given population, whose characteristics could thus be modified by the addition, deletion, editing or even suppression of certain genes.

Gene drives present an unprecedented opportunity to cure some of the most devastating risks to health and the environment. Applications are foreseen in the fight against malaria and other insect-borne diseases, which the reprogramming of mosquito genomes could potentially eliminate from entire regions. They are also foreseen in combating herbicide and pesticide resistance, and in eradicating invasive species that threaten the biodiversity of ecosystems.

Technical challenges remain, relating mainly to the difficulty of editing genomes for programming drives in a way that is precise (with only the targeted gene affected) and reversible (to prevent and overwrite possible unwanted changes). A team at Harvard University, MIT and the University of California at Berkeley is making huge progress, such that the development of purpose-built, engineered gene drives is expected in the next few years.

However, gene drives carry potential risks to wild organisms, crops and livestock: unintentional damage could possibly be triggered and cascade through other connected ecosystems. No clear regulatory framework to deal with gene drives currently exists. The US Food and Drug Administration would consider them as veterinary medicines, requiring the developers to demonstrate they are safe for animals that need to be protected. So how are they defined? Both the US policy on Dual Use Research of Concern, which oversees research that has clear security concerns, and the Australia Group Guidelines, a form of private regulations on transfers of biological material, rely on lists of infectious bacterial and viral agents. They do not have the functional approach that would be needed, for example, to regulate genetic modifications to sexually reproducing plants and animals.

Scientists and regulators need to work together from an early stage to understand the challenges, opportunities and risks associated with gene drives, and agree in advance to a governance regime that would govern research, testing and release. Acting now would allow time for research into areas of uncertainty, public discussion of security and environmental concerns, and the development and testing of safety features. Governance standards or regulatory regimes need to be developed proactively and flexibly to adapt to the fast-moving development of the science.

Sources: Esvelt et al. 2014 and Oye et al. 2014.

Notes:
1 Begun in particular by Prof. Austin Burt, Imperial College London.
2 CRISPR-Cas9 is a tool that aims to accelerate the technology to edit genomes. It enables an organism’s DNA to be rewritten.

issue as innovations become more interdisciplinary and technologies converge. Examples include Google Glass, autonomous cars and M-healthcare: while all rely on Internet standards, they also have ramifications in other spheres. Often no mechanism exists for deciding which existing regulatory body, if any, should take responsibility for an emerging technology.

Striking a balance between precaution and innovation is an overall dilemma. Often potentially-beneficial innovations cannot be tested without some degree of risk. For example, a new organism may escape into the environment and cause damage. Weighing risks against benefits involves attempting to anticipate the issues of tomorrow and deciding how to allocate scarce regulatory resources among highly technical fields.

When a gap in governance exists, it may create a vacuum of power that could be filled by religious movements and action groups exerting more influence and potentially stifling innovation. With that risk in mind, industry players in emerging technologies where institutions are weak or non-existent may seek to respond to a governance gap by demonstrating their responsibility through self-regulating – as the “biohacker” community is attempting in synthetic biology. Another example of a private player highlighting a governance gap is the way Facebook effectively exerts regulatory power in online identity management and censorship, through policies such as forcing users to display their real names and removing images that it believes the majority of users might find offensive.
Artificial Intelligence (AI) is the discipline that studies how to create software and systems that behave intelligently. AI scientists build systems that can solve reasoning tasks, learn from data, make decisions and plans, play games, perceive their environments, move autonomously, manipulate objects, respond to queries expressed in human languages, translate between languages, and more.

AI has captured the public imagination for decades, especially in the form of anthropomorphized robots, and recent advances have pushed AI into popular awareness and use: IBM’s “Watson” computer beat the best human Jeopardy! players; statistical approaches have significantly improved Google’s automatic translation services and digital personal assistants such as Apple’s Siri; semi-autonomous drones monitor and strike military targets around the world; and Google’s self-driving car has driven hundreds of thousands of miles on public roads.

This represents substantial progress since the 1950s, and yet the original dream of a machine that could substitute for arbitrary human labour remains elusive. One important lesson has been that, as Hans Moravec wrote in the 1980s, “it is comparatively easy to make computers exhibit adult level performance on intelligence tests or playing checkers, and difficult or impossible to give them the skills of a one-year-old when it comes to perception and mobility”.

These and other challenges to AI progress are by now well known within the field, but a recent survey shows that the most-cited living AI scientists still expect human-level AI to be produced in the latter half of this century, if not sooner, followed (in a few years or decades) by substantially smarter-than-human AI. If they are right, such an advance would likely transform nearly every sector of human activity.

If this technological transition is handled well, it could lead to enormously higher productivity and standards of living. On the other hand, if the transition is mishandled, the consequences could be catastrophic. How might the transition be mishandled? Contrary to public perception and Hollywood screenplays, it does not seem likely that advanced AI will suddenly become conscious and malicious. Instead, according to a co-author of the world’s leading AI textbook, Stuart Russell of the University of California, Berkeley, the core problem is one of aligning AI goals with human goals. If smarter-than-human AIs are built with goal specifications that subtly differ from what their inventors intended, it is not clear that it will be possible to stop those AIs from using all available resources to pursue those goals, any more than chimpanzees can stop humans from doing what they want.

In the nearer term, however, numerous other social challenges need to be addressed. In the next few decades, AI is anticipated to partially or fully substitute for human labour in many occupations, and it is not clear whether human workers can be retrained quickly enough to maintain high levels of employment. What is more, while previous waves of technology have also created new kinds of jobs, this time structural unemployment may be permanent as AI could be better than humans at performing the new jobs it creates. This may require a complete restructuring of the economy by raising fundamental questions of the nature of economic transactions and what it is that humans can do for each other. Autonomous vehicles and other cases of human-robot interaction demand legal solutions fit for the novel combination of automatic decision-making with a capacity for physical harm. Autonomous vehicles will encounter situations where they must weigh the risks of injury to passengers against the risks to pedestrians; what will be the legal redress be for parties who believe the vehicle decided wrongly? Several nations are working towards the development of lethal autonomous weapons systems that can assess information, choose targets and open fire without human intervention. Such developments raise new challenges for international law and the protection of non-combatants. Who will be accountable if they violate international law? The Geneva Conventions are unclear. It is also not clear when human intervention occurs: before deployment, during deployment? Humans will be involved in programming autonomous weapons; the question is whether human control of the weapon ceases at the moment of deployment. AI in finance and other domains has introduced risks associated with the fact that AI programmes can make millions of economically significant decisions before a human can notice and react, leading for example to a May 2012 trading event that nearly bankrupted Knight Capital.

In short, proactive and future-oriented work in many fields is needed to counteract “the tendency of technological advance to outpace the social control of technology”.

Notes:
1 Moravec, 1988, p. 15.
2 Müller and Bostrom, 2014.
3 Bostrom, 2014.
4 Omohundro, 2008.
5 Brynjolfsson and McAfee, 2014.
8 Johnson et al., 2013.
A fundamental question pertains to societal, economic and ethical implications. While emerging technologies imply the long-term possibility of a world of abundance, many countries are struggling with unemployment and underemployment, and even a temporary adjustment due to technological advancement could undermine social stability. In ethical terms, advances in transhumanism, using technology to enhance human physiology and intelligence, will require finding a definition for what people mean by human dignity; are enhanced human capabilities a basic human right, or a privilege for those who can pay, even if that exacerbates and entrenches inequalities? At the same time, governance regimes for emerging technologies are strongly influenced by the perceptions, opinions and values of society – whether people are more enthusiastic about a technology’s potential benefits than fearful about its risks. This is very domain-related, and not always rational or proportional: it can lead to some technologies being over-regulated and others under-regulated. Many biological technologies that touch on beliefs about religion and human life, for example, are regulated relatively stringently, as evidenced by the worldwide prohibition on human cloning. On the other hand, the human propensity to anthropomorphize means that robotic prototypes in some empathic form of assistive technology (such as Paro, a baby harp seal lookalike robot assisting in the care of people with dementia and other health problems) easily capture public sympathy, which may ease safety, ethical or legal concerns. In other areas, such as lethal autonomous weapons, it would probably be easier to get close to unanimous public support to prohibit them as has been the case for landmines. As such, these societal implications constitute an important risk in themselves, as it is difficult to anticipate their impact on the use and path of emerging technologies.

**Thoughts for the Future**

Emerging technologies are developing rapidly. Their far-reaching societal, economic, environmental and geopolitical implications necessitate a debate today to chart the course for the future and reap the many benefits but avoid the risks of emerging technologies. This is not a trivial task given the many interdependencies and uncertainties and the fact that many challenges transcend the spheres of decision-makers both across technologies and borders. Regulators face the dilemma to design regulatory systems that are predictable enough for companies, investors and scientists to make rational decisions, but unambiguous enough to avoid a governance gap that could jeopardize public consent or give too much room to non-state actors. Against this backdrop, evolving and adaptive regulatory systems should be designed in a flexible manner to take into account changing socio-economic conditions, new scientific insights and the discovery of unknown interdependencies.

In light of the complexities and rapidly changing nature of emerging technologies, governance should be designed in such a way as to facilitate dialogue among all stakeholders. For regulators, to dialogue with researchers at the cutting edge of developing these technologies is the only way to understand the potential future implications of new and highly-technical capabilities. For the scientific community within and across certain fields, a safe space is needed to coalesce around a common language and have an open discussion around both benefits and risks. At the same time, given that risks tend to cross borders, so must the dialogue on how to respond. And given the power of public opinion to shape regulatory responses, the general public must also be included in an open dialogue about the risks and opportunities of emerging technologies through carefully-managed communication strategies. Governance will be more stable and less likely either to overlook emerging threats or to stifle innovation unnecessarily, if the various stakeholders likely to be affected are involved in the thinking about potential regulatory regimes and given the knowledge to enable them to make informed decisions.

**2.5 Conclusion**

Although the interplay between geopolitics and economics, urbanization and emerging technologies are three very different fields of enquiry, two common themes emerge: the importance of governance and the need for proactivity.

The analysis of the interplay between geopolitics and economics focuses attention on the need to find ways to minimize incentives for national governments to engage in negative tactics, including by making the mechanisms of global governance more effective in resolving tensions among nation states. As this interplay leads to regional institutions gaining in significance, proactive attention to the quality and effectiveness of their governance also becomes more important in creating the capacity to address risks.

There is no doubt that urbanization will continue, so improving the governance of cities will be relevant to a broad spectrum of global risks. An opportunity also exists to be proactive in fostering more effective links between city governments around the world, for mutual learning and collaboration on risks that affect them.

Emerging technologies promise to play a leading role in improving the governance of smart cities, but also present risks. Proactivity is especially crucial here given that the risks that might emerge from entirely new fields of knowledge are impossible to predict. Effective governance at all levels, from industry codes of conduct to national regulations and global cooperation, will determine how well risks from emerging technologies are foreseen and minimized.
Endnotes

5 McKinsey Global Institute, 2011.
13 Alirol et al., 2011.
15 Hawkins et al., 2013.
17 Alirol et al., 2011.
18 World Health Organization, 2014b.
19 Alirol et al., 2011.
20 Alirol et al., 2011.
22 IDF, 2013.
23 IDF, 2013.
24 Alirol et al., 2011.
26 IDF, 2013.
27 IDF, 2013.
28 Ramachandran et al., 2008.
29 IDF, 2013.
30 IDF, 2013.
31 Ramachandran et al., 2008.
32 Ramachandran et al., 2008.
34 IDF, 2013.
35 Ramachandran et al., 2008.
36 IDF, 2013.
37 Ramachandran et al., 2008.
38 New Climate Economy, 2014.
Part 3: Good Practices on Risk Management and Risk Resilience

Introduction

Mitigating, preparing for and building resilience against global risks is a long and complex process, a necessity often recognized in theory but difficult in practice. Global risks transcend borders, meaning that often no single entity has the capacity and authority to address them. Multistakeholder collaboration is required but made difficult by misaligned incentives and uncertainties – those with the most to lose from a risk are often not those with the most power to address it. And the highly interconnected nature of global risks means they need to be addressed from multiple angles – although this also means that investments in risk mitigation and resilience can pay off in multiple areas.

Analysing and better understanding global risks is the first step towards successful efforts to address them. Risks must be effectively communicated to the public, government, business and civil society. Even then, action is more likely to happen if stakeholders have examples of good practice on which to draw. With that in mind, this year’s Global Risks report shares three examples of risk management and resilience practices related to extreme weather events.

The focus on extreme weather events is pertinent given that it tied with large-scale involuntary migration at the bottom of the list when respondents to the Global Risks Perception Survey 2014 were asked to rate what progress had been made in addressing each global risk over the past 10 years (see Figure 3.1). Water crises and risks related to extreme weather events, such as natural disasters, major biodiversity loss and ecosystem collapse, are also in the bottom half of responses. In addition, water crises is the global risk that is perceived as the most potentially impactful in the coming decade (see Figure 1).

The impact of natural hazards is a combination of the frequency and intensity of the hazard with the vulnerability and exposure of people, assets and economic activities. Strengthening resilience is an attempt to reduce the exposure and ultimately the potentially catastrophic impact of natural hazards.
The first practice presented here addresses water crises. In the coming decades, climate change will add to the pressure that economic growth and development are already putting on both groundwater and renewable surface water resources. As water is an issue that must be managed locally, proven local initiatives that can be adapted and replicated elsewhere are needed. The initiative described here was developed in Australia’s Murray-Darling Basin and has been transferred in other regions of Asia.

Community-level action to build resilience is the focus of the second practice outlined below, the newly-established Resilient America Roundtable. This highly promising initiative is helping selected local communities in the United States to understand their risk interconnections and design resilience strategies against risks, including extreme weather events. It is hoped that the lessons learned will enable many more communities to do the same.

The importance of adequate risk communication is a recurring theme in effective risk management practices, and it is at the heart of the third practice presented here – on raising public awareness about flood risks in Saxony, a region of Germany that is prone to significant flooding (ZÜRS Public).

The examples showcased here are not intended to be exhaustive; they are selected sources of inspiration and a base for continuing this work in the future.

---

**Figure 3.1: Global Risks for Which Most Progress Has Been Made within the Last 10 Years**

<table>
<thead>
<tr>
<th>Economic risks</th>
<th>24.3%</th>
<th>23.3%</th>
<th>26.4%</th>
<th>26.3%</th>
<th>10.9%</th>
<th>15.9%</th>
<th>14.4%</th>
<th>5.7%</th>
<th>5.2%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure of financial mechanism or institution</td>
<td>24.3%</td>
<td>23.3%</td>
<td>26.4%</td>
<td>26.3%</td>
<td>10.9%</td>
<td>15.9%</td>
<td>14.4%</td>
<td>5.7%</td>
<td>5.2%</td>
</tr>
<tr>
<td>Unmanageable inflation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fiscal crisis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Energy price shock</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset bubble</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deflation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unemployment or underemployment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure of critical infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Societal risks</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Spread of infectious diseases</td>
<td>16.6%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Food crises</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure of urban planning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Water crises</td>
<td>6.8%</td>
<td>11.3%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Profound social instability</td>
<td>3.3%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large-scale involuntary migration</td>
<td>3.3%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technological risks</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical information infrastructure breakdown</td>
<td>16.8%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber attacks</td>
<td>6.8%</td>
<td>11.3%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data fraud or theft</td>
<td>3.3%</td>
<td>6.8%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Misuse of technologies</td>
<td>3.3%</td>
<td>6.8%</td>
<td>11.3%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Environmental risks</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure of climate-change adaptation</td>
<td>6.8%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Man-made environmental catastrophes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biodiversity loss and ecosystem collapse</td>
<td>6.5%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Natural catastrophes</td>
<td>3.3%</td>
<td>6.8%</td>
<td>11.3%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extreme weather events</td>
<td>3.3%</td>
<td>6.8%</td>
<td>11.3%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Source:** Global Risks Perception Survey 2014, World Economic Forum.  
Note: Respondents were asked to select three global risks for which they believe most progress has been made to address them within the last 10 years. For legibility reasons, the names of the global risks are abbreviated. See Appendix A for the full name and description.
Part 1

Practice 1: Interdisciplinary Science for Managing Water Resources and Improving Long-Term Water Security

Securing a reliable supply of clean water has been one of the most important issues throughout human history. Water management involves mitigating four risks: shortages, including droughts; inadequate quality; flooding; and harming ecological systems. According to the United Nations:

♦ Water use is growing at twice the pace of population growth. By 2025, two-thirds of the world population will be experiencing water "stress conditions".

♦ One in nine people lacks access to improved sources of drinking water and one in three lacks improved sources of water sanitation. This causes around 3.5 million deaths each year.

♦ Between 2000 and 2006, droughts, floods and storm surges killed almost 300,000 people and caused an estimated $422 billion worth of damage.

Climate change will increase the frequency and severity of droughts and floods and will lead to overall drier conditions in some world regions. This may heighten the risk of geopolitical destabilization and armed conflict: countries that share rivers have a statistically higher likelihood of armed conflict, and dry countries experience more conflict. The Jordan, Rio Grande, Mekong and Nile rivers are all especially associated with conflict risk.

The Murray-Darling Basin

Australia's Murray-Darling Basin provides water for over 2 million people, including much of the city of Adelaide, as well as 40% of Australia's agriculture. Unsustainable rates of water extraction had been decreasing flow volumes: in 2007, the car ferry at the River Murray mouth was grounded for the first time in its 71-year history.

There was a growing sense that something had to be done to ensure that the river system was not destroyed. Policy-makers realized that they urgently required a model that could provide credible and robust estimates of current and future water availability, to enable them to set equitable and efficient allocations for competing uses. However, such a model had not yet been designed, let alone built.

The complexity of modelling an entire river system – which requires handling vast amounts of often incomplete data from multiple sources of varying accuracy and reliability – had been insurmountable until recently. But prior investments in fields such as hydrology, mathematics, climate and statistics had paid off in the shape of advances that were making such a model possible. Then-prime minister John Howard identified it as a national priority and committed government funding.

First, climate patterns as well as individual models of groundwater and surface water inflows and outflows had to be developed, for different parts of an area larger than France. Then these individual models had to be brought together into a single, integrated model. Starting in 2006, a team of around 100 people from 15 organizations developed ways to handle the uncertainties and link the models. The resulting system incorporated 70 individual ground and surface water models and over a century of climate data into a 61,000 gigabyte database – roughly the size of the US Library of Congress.

The project combined both blue-sky and applied research. It involved the development of new techniques for hydrological, environmental and climate modelling, with transparency and expert review to validate methods and build stakeholder trust. The project is the first rigorous attempt worldwide to estimate the impacts of catchment development, changing groundwater extraction, climate variability and anticipated climate change, on water resources at a basin-scale, explicitly considering the connectivity of surface and groundwater systems.

Today the Murray-Darling Basin Authority – a government organization charged with managing the basin’s water resources – provides a real-time interactive website where anyone can view daily and yearly water levels, salt loads (electrical conductivity) and water temperatures at recording stations for all the basin’s major rivers. This provides traceability and transparency for critical decisions relating to water allocation. In a multistakeholder environment where allocation decisions can impact people’s livelihoods, trust in the data is critical for effective policy.

Figure 3.2: The Murray-Darling Basin in Australia

Source: CSIRO Land and Water Flagship
Next-Generation Models

The general principles of the technologies pioneered in the Murray-Darling Basin are applicable to other river systems, although they need to be adapted to the unique environmental features of each. This is now happening for the Mekong River Basin, one of the largest in the world, which covers China, Myanmar, Lao PDR, Thailand, Cambodia and Vietnam: over 60 million people depend on the Mekong for their water supply, and many hydropower plants are planned or under construction.

The science of river basin planning is also advancing to incorporate social science alongside the physical sciences in efforts to improve the resilience of social, economic and environmental systems. In a 2010 study with funding from the Australian overseas aid agency, the Commonwealth Scientific and Industrial Research Organisation (CSIRO) and the Mekong River Commission developed six scenarios for the Mekong Basin to the year 2050. The Mekong Futures Project sought to understand the complex transboundary regional dynamics to improve decision-making, ensure participatory processes and develop shared future visions. The CSIRO team working on the project had both physical and socio-economic science backgrounds.10

Another project will see yet more advanced techniques applied to model water availability, ecosystems and livelihoods for the Koshi River Basin, which stretches from China across the Himalayas, through Nepal and into the Ganges in India. In 2013, CSIRO commenced a collaborative four-year project with the International Centre for Integrated Mountain Development to inform transboundary water reforms.11 Reliable information about how much water can be safely extracted from a river system is vital to help countries reach agreements on long-term water security.

As the models increase in sophistication, the challenge is to plug them into real-world decision-making processes. Building the models is hard, but so too is convincing policymakers to act on them when they point towards the need to make difficult choices.

Practice 2: Resilient America Roundtable

Floods, hurricanes, wildfires, windstorms and other natural hazards kill or injure thousands of people worldwide and cost billions of dollars in the United States each year. The factors that make a community resilient against these threats – able to protect against, absorb, mitigate, respond to or recover from them – differ greatly according to local circumstances. But many communities have not even begun to think about how to assess their resilience, let alone build it.

Started in January 2014, the Resilient America Roundtable initiative by the National Academy of Sciences aims to work with communities in a bottom-up way. Over a three-year time horizon, the purpose of the initiative is to initiate, nurture and learn from local efforts to measure and improve resilience. It emerged from interest in testing ideas included in the 2012 US National Research Council report entitled Disaster Resilience: A National Imperative on reducing vulnerability to extreme events, decreasing their costs and mitigating their impacts. The Resilient America Roundtable has a strong multistakeholder component: initiated by nine federal agencies, it convenes experts from the academic, public and private sectors. The science community is represented by the National Academy of Sciences.

The Resilient America Roundtable has designed and is currently catalysing pilot projects in communities in South Carolina, Seattle/Tacoma and Iowa, thus offering a geographic representation by ranging from the west (Seattle/Tacoma) to the middle (Iowa) to the east (South Carolina). The communities were selected based on criteria including their size, ethnic and economic diversity, the range and type of natural hazard risks they face and the presence of motivated community leadership to own and maintain the resulting community resilience strategy in the long term. The pilot projects are structured around four pillars: (i) understanding and communicating risk; (ii) identifying measures or metrics of resilience, including baseline conditions, milestones and definitions of the acceptable or unacceptable consequences of the identified risks; (iii) building or strengthening coalitions or partnerships in building community resilience; and (iv) sharing information or data related to better decision-making for building resilient communities.

The pilot project initially involves five steps, the first two of which have been implemented. First, a Roundtable subcommittee makes visits to engage different community groups including the business community – local corner stores as well as multinational chains; local government agencies; emergency managers and first responders; and the local chapters of community-based non-governmental organizations such as the American Red Cross, the United Way, Points of Light and the Boys & Girls Clubs of America. Separate discussions are held with each about their views on resilience and what elements of quality of life must be maintained during emergency. Around 70-100 people have participated in these conversations so far in Iowa and South Carolina.

Second, 70 people are invited to play a specially-developed “Extreme Events” game, in which everyone chooses a role (first responder, individual, elected official, etc.) in a fictional Coastal City and makes decisions as a scripted scenario unfolds that involves a hurricane and other surprises. The game takes the players through the efforts of finding, sharing and distributing resources. Its purpose is to break the ice and build trust among the members of each community. The game will also be made available online.

Third, a set of interactive table top exercises will be developed to understand and map the specific interdependencies in each community. The pilots have identified certain “community priorities” as a basis for this exercise: in Charleston and Iowa, economic drivers have emerged as community priorities; in Charleston, priorities include cultural identity and tourism and, in Iowa, the thrust is on grain production and export.

Fourth, the community participants will be helped to work through a scenario of a disrupting event in which critical infrastructure fails. The goal is to highlight critical nodes, networks and functions that act as amplifiers or dampeners as the effects of a disrupting event cascade through the system. Finally, the resulting disruption map will identify the nodes...
that require hardening or redundancy and that will be used as a basis to design the community’s resilience strategy.

In terms of barriers, the initiative relates to two overarching objectives: to build resilience at the community level; and, at a higher level, to gain insights into common themes and local variations on those themes to knit into a national or a larger-scale picture. Concerning the latter, the main challenge has, therefore, been to structure the pilot projects in such a way as to be able to glean common elements or themes from disparate communities. By using the same basic approach (the four pillars) in each community and seeing which elements of the framework play out, it is possible to understand the similarities and differences in how to build resilience and whether there are enough common issues that could be used as a basis to transfer the project to other communities. The big barrier for transferability would be if one were to find through the small sample that each community builds resilience in its own ways and that few or weak ties bind communities together.

Project-wise, the experience has shown so far that one of the main enabling factors for building community resilience to all kinds of risks is for the community to be functional and for the different pieces of that community to work together in a productive way. While a collegial and cooperative approach prevails in some communities from the outset, in others more time needs to be spent to build trust among different sectors and stakeholders. In addition, the key to maintaining momentum is local leadership: having somebody – whether an individual, an agency or an organization – take ownership of the community resilience strategy in a way that allows it to be resourced and maintained over time.

The Resilient America website (http://resilientamerica.nas.edu) facilitates connections among the three pilot and other communities and will share the resulting information and lessons learned. It is hoped that the Resilient America Roundtable’s emphasis on risk communication and inclusive understanding of resilience will ultimately spark ideas for similar initiatives in other communities or countries.

Practice 3: ZÜRS Public – Increasing Awareness of Flood Risk in Saxony – A Practice on Risk Communication

In August 2002, severe floods affected practically two-thirds of the German state of Saxony (Figure 3.3 illustrates the rivers in Saxony, Germany). This disastrous event led to the development of the Flood Protection Investment Programme, which comprises 1,600 individual flood protection measures and 548 flood risk maps for all communities at risk. A statewide risk awareness campaign was also launched.

To better communicate on flood risks, in collaboration with the Ministry of Saxony, the German Insurance Association (GDV) developed an online geographic information system, ZÜRS Public, where homeowners, tenants and businesses can see an exact calculation of the risk exposure to flooding, backflow, torrential rain and earthquakes of their individual address. While similar to other systems, such as Tiris in the Austrian region of Tyrol, it is innovative in its triangulation of data from insurers, the government and some 200 water management agencies across the federal states. The results of this online risk information tool are easy to understand and free of charge.

Since its establishment in 2001, the ZÜRS Public online risk assessment tool has covered some 20 million home addresses, 200,000 km of rivers, and is available in Saxony, Lower Saxony and Saxony-Anhalt. The GDV is working to develop it into a standardized tool for all of Germany. Currently the tool is being developed in Rhineland-Palatinate and Bavaria. Flood risk calculations are presented in four groups:

♦ high threat: statistically, floods occur at least once every 10 years
♦ medium threat: statistically, floods occur once every 10-50 years
♦ low threat: statistically, floods occur once every 50-200 years
♦ very low threat: statistically, floods occur less frequently than once every 200 years

The initiative aligned the interests of all stakeholders and illustrates the importance of risk communication. Citizens benefit by understanding more about their individual risk exposure. The insurance industry is incentivized to participate as the tool encourages households and businesses to think about their need for insurance. The state also benefits from individuals and businesses taking greater responsibility for risk prevention, both through private insurance and investment in physical prevention measures, as it reduces their potential liability in the event of disasters. To raise awareness further, the state government transparently publishes information online about applications for and disbursements of public compensation for private damages.

Figure 3.3: The Rivers in Saxony, Germany
Conclusion

The three practices described in this section of the report illustrate how risk mitigation and resilience-building efforts can be driven by one stakeholder or can progress through a broad-based multistakeholder coalition. From an emphasis on data collection and analysis in the case of the Murray-Darling Basin, to community building around resilience in the United States and risk communication in Germany, they show how responses to environmental risks can be based at the community, regional or national levels, and highlight the importance of knowledge and capability transfer.

Building resilience means finding ways to change behaviours across sectors and systems, identifying the barriers that must be addressed and the enablers that should be leveraged. Readers of the Global Risks report are invited to submit suggestions for practices on risk management or risk resilience to be featured in future editions of the report.

Endnotes

1. Resilience is the ability of households, communities and nations to absorb and recover from shocks, while positively adapting and transforming their structures and means for living in the face of long-term stresses, change and uncertainty (Mitchell, 2013).
2. IPCC, 2014.
4. UN Water, 2013. UN-Water Thematic Factsheets.
7. Gleditsch et al., 2006.
15. See http://www.gdv.de/2013/06/zuers-public/.

References

Conclusion

Our lives are very different today from when the first Global Risks report was published a decade ago. Little did the world imagine the possibility of the implosion of global financial markets that plunged the world into a socio-economic crisis from which it is still struggling to emerge. The “real world” was nowhere near as interconnected with the virtual one: Twitter did not exist, Facebook was still a student-only service, and the iPhone and Android were still one and two years, respectively, away from their commercial release. The power of interconnectivity has since shown itself forcefully – be it from the convening power of the Arab Spring, the revelation of massive cyber espionage around the National Security Agency, or fast-moving developments in new disruptive business models that are fundamentally changing the global economic landscape.

While increased interdependencies have brought the world closer together, the Global Risks report series emphasizes the other side of the coin: as people’s lives are becoming more complex and more difficult to manage, businesses, governments and individuals alike are being forced to decide upon courses of action in an environment clouded by multiple layers of uncertainty. Indeed, understanding their implications and raising awareness of the interconnection of risks are at the basis of the Global Risks report. On the upside, however, the world has not stood still: the importance of risk management and the need to build resilience has since become a top issue for decision-makers who are recognizing that risks are no longer isolated but inherently dynamic in nature and crossing many spheres of influence. Against this backdrop, the need to collaborate and learn from each other is clearer than ever, an aspect that figures prominently in this year’s report by featuring initiatives that have demonstrated value and good practices that can be replicated elsewhere.

Ten years of “doing risks” has also led to the recognition that a short-term vision prevents addressing long-term issues. Some slower-moving trends have continued inexorably: the last 10 years have brought conclusive proof that the earth’s climate is changing and that human activities are to blame – yet
progress to mitigate greenhouse gas emissions remains frustratingly slow. This lesson is reflected this year in the introduction of different time horizons and the differentiation between risks and trends. Hopefully these innovations will help many public and private organizations around the world address this aspect of human nature in mitigating risks and building resilience.

Indeed, our self-perception as *hominis economici* or rational beings has faltered in the aftermath of the financial crisis, whose effects are still unfolding socially, as persistent unemployment, ever-rising inequality, unmanaged migration flows and ideological polarization are among the factors stretching societies dangerously close to the breaking point. Social fragility is even threatening geopolitical stability, as breakdowns in cooperation within states make relations between states more difficult. And a quarter-century after the fall of the Berlin Wall, interstate conflict is once again one of the key risks in terms of likelihood and impact. Yet the means through which conflicts can be pursued are growing more varied, as this report has explored – from geo-economic tools, such as trade sanctions, to cyber attacks on critical infrastructure, to the potential for a new arms race in lethal autonomous weapons systems.

We are not powerless in the face of these concerns. As highlighted previously, multistakeholder collaboration and global governance are key to building resilience and mitigating risks. From major intergovernmental conferences in Sendai and Paris to the finalization of the Sustainable Development Goals, the year 2015 presents an unprecedented range of opportunities to take collective action to address global risks.
Appendices
## Appendix A: Description of Global Risks and Trends 2015

### Global Risks

A global risk is defined as an uncertain event or condition that, if it occurs, can cause significant negative impact for several countries or industries within the next 10 years.

### Table A.1: Description of Global Risks 2015

<table>
<thead>
<tr>
<th>Global Risk</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset bubble in a major economy</td>
<td>Unsustainably overpriced assets, such as commodities, housing, shares, etc., in a major economy or region</td>
</tr>
<tr>
<td>Deflation in a major economy</td>
<td>Prolonged ultra-low inflation or deflation in a major economy or region</td>
</tr>
<tr>
<td>Energy price shock to the global economy</td>
<td>Sharp and/or sustained energy price increases that place further economic pressures on highly energy-dependent industries and consumers</td>
</tr>
<tr>
<td>Failure of a major financial mechanism or institution</td>
<td>Collapse of a financial institution and/or inefficient functioning of a financial system with implications throughout the global economy</td>
</tr>
<tr>
<td>Failure/shortfall of critical infrastructure</td>
<td>Failure to adequately invest in, upgrade and secure infrastructure networks leads to a breakdown with system-wide implications</td>
</tr>
<tr>
<td>Fiscal crises in key economies</td>
<td>Excessive debt burdens generate sovereign debt crises and/or liquidity crises</td>
</tr>
<tr>
<td>High structural unemployment or underemployment</td>
<td>A sustained high level of unemployment or underutilization of the productive capacity of the employed population</td>
</tr>
<tr>
<td>Unmanageable inflation</td>
<td>Unmanageable increase in the general price level of goods and services in key economies</td>
</tr>
<tr>
<td>Extreme weather events (e.g. floods, storms, etc.)</td>
<td>Major property, infrastructure and environmental damage as well as human loss caused by extreme weather events</td>
</tr>
<tr>
<td>Failure of climate-change adaptation</td>
<td>Governments and businesses fail to enforce or enact effective measures to protect populations and to help businesses impacted by climate change to adapt</td>
</tr>
<tr>
<td>Major biodiversity loss and ecosystem collapse (land or ocean)</td>
<td>Irreversible consequences for the environment resulting in severely depleted resources for humankind as well as industries such as fishing, forestry, pharmaceuticals</td>
</tr>
<tr>
<td>Major natural catastrophes (e.g. earthquake, tsunami, volcanic eruption, geomagnetic storms)</td>
<td>Major property, infrastructure and environmental damage as well as human loss caused by geophysical disasters such as earthquakes, volcanic activity, landslides, tsunamis or geomagnetic storms</td>
</tr>
<tr>
<td>Man-made environmental catastrophes (e.g. oil spill, radioactive contamination, etc.)</td>
<td>Failure to prevent major man-made catastrophes causing harm to lives, human health, infrastructure, property, economic activity and the environment</td>
</tr>
<tr>
<td>Global Risk Description</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Failure of national governance (e.g. corruption, illicit trade, organized crime, impunity, political deadlock, etc.)</td>
<td>Inability to efficiently govern a nation of geopolitical importance due to weak rule of law, corruption, illicit trade, organized crime, impunity or political deadlock</td>
</tr>
<tr>
<td>Interstate conflict with regional consequences</td>
<td>A bilateral or multilateral dispute between states escalates into economic (e.g. trade/currency wars, resource nationalization), military, cyber, societal or other conflict</td>
</tr>
<tr>
<td>Large-scale terrorist attacks</td>
<td>Individuals or non-state groups with political or religious goals successfully inflict large-scale human or material damage</td>
</tr>
<tr>
<td>State collapse or crisis (e.g. civil conflict, military coup, failed states, etc.)</td>
<td>State collapse of geopolitical importance due to internal violence, regional or global instability and military coup, civil conflict, failed states, etc.</td>
</tr>
<tr>
<td>Weapons of mass destruction</td>
<td>Nuclear, chemical, biological and radiological technologies and materials are deployed creating international crises and potential for significant destruction</td>
</tr>
<tr>
<td>Failure of urban planning</td>
<td>Poorly planned cities, urban sprawl and associated infrastructure create social, environmental and health challenges</td>
</tr>
<tr>
<td>Food crises</td>
<td>Access to appropriate quantities and quality of food and nutrition becomes inadequate, unaffordable or unreliable on a major scale</td>
</tr>
<tr>
<td>Large-scale involuntary migration</td>
<td>Large-scale involuntary migration due to conflict, disasters, environmental or economic reasons</td>
</tr>
<tr>
<td>Profound social instability</td>
<td>Major social movements or protests (e.g. street riots, social unrest, etc.) disrupt political or social stability, negatively impacting populations and economic activity</td>
</tr>
<tr>
<td>Rapid and massive spread of infectious diseases</td>
<td>Bacteria, viruses, parasites or fungi cause uncontrolled spread of infectious diseases (for instance due to resistance to antibiotics, antivirals and other treatments), leading to widespread fatalities and economic disruption</td>
</tr>
<tr>
<td>Water crises</td>
<td>A significant decline in the available quality and quantity of fresh water, resulting in harmful effects on human health and/or economic activity</td>
</tr>
<tr>
<td>Breakdown of critical information infrastructure and networks</td>
<td>Systemic failures of critical information infrastructure (e.g. Internet, satellites, etc.) and networks negatively impact industrial production, public services and communications</td>
</tr>
<tr>
<td>Large-scale cyber attacks</td>
<td>State-sponsored, state-affiliated, criminal or terrorist large-scale cyber attacks cause an infrastructure breakdown and/or loss of trust in the Internet</td>
</tr>
<tr>
<td>Massive incident of data fraud/theft</td>
<td>Criminal or state-sponsored wrongful exploitation of private or official data takes place on an unprecedented scale</td>
</tr>
<tr>
<td>Massive and widespread misuse of technologies (e.g. 3D printing, artificial intelligence, geo-engineering, synthetic biology, etc.)</td>
<td>Massive and widespread misuse of technologies, such as 3D printing, artificial intelligence, geo-engineering and synthetic biology, causing human, environmental and economic damage</td>
</tr>
</tbody>
</table>
**Trends**

A trend is defined as a long-term pattern that is currently taking place and that could contribute to amplifying global risks and/or altering the relationship between them.

**Table A.2: Description of Trends 2015**

<table>
<thead>
<tr>
<th>Trend</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ageing population</td>
<td>Ageing of populations in developed and developing countries driven by declining fertility and decrease of middle- and old-age mortality</td>
</tr>
<tr>
<td>Climate change</td>
<td>Change of climate attributed directly or indirectly to human activity that alters the composition of the global atmosphere and which is in addition to natural climate variability</td>
</tr>
<tr>
<td>Environmental degradation</td>
<td>Deterioration in quality of air, soil and water from ambient concentrations of pollutants and other activities and processes</td>
</tr>
<tr>
<td>Growing middle class in emerging economies</td>
<td>Growing share of population reaching middle-class income levels in emerging economies</td>
</tr>
<tr>
<td>Increasing national sentiment</td>
<td>Increasing national sentiment among populations and political leaders affecting countries’ national and international political positions</td>
</tr>
<tr>
<td>Increasing polarization of societies</td>
<td>Inability to reach agreement on key issues within countries due to diverging or extreme values, political or religious views</td>
</tr>
<tr>
<td>Rise of chronic diseases</td>
<td>Increasing rates of non-communicable diseases, also known as chronic diseases, leading to long-term costs of treatment threatening recent societal gains in life expectancy and quality, placing a burden on economies</td>
</tr>
<tr>
<td>Rise of hyperconnectivity</td>
<td>Increasing digital interconnection of people and things</td>
</tr>
<tr>
<td>Rising geographic mobility</td>
<td>Increasing mobility of people and things due to quicker and better performing means of transport and lowered barriers</td>
</tr>
<tr>
<td>Rising income disparity</td>
<td>Increasing socio-economic gap between rich and poor in major countries or regions</td>
</tr>
<tr>
<td>Shifts in power</td>
<td>Shifting power from state to non-state actors and individuals, from global to regional levels, and from developed to emerging market and developing economies</td>
</tr>
<tr>
<td>Urbanization</td>
<td>Rising number of people living in urban areas, resulting in the physical growth of cities</td>
</tr>
<tr>
<td>Weakening of international governance</td>
<td>Weakening or inadequate global or regional institutions’ (e.g. the UN, IMF, NATO, etc.) agreements or networks, and loss of trust in them, increasing the global power vacuum and preventing effective solutions to global challenges</td>
</tr>
</tbody>
</table>
Appendix B: The Global Risks Perception Survey 2014 and Methodology

As discussed in Part 1, the Global Risks 2015 methodology was reviewed last year for this edition. A number of workshops, interviews and discussions were held with experts and with the Advisory Board, taking into account lessons from past editions as well as developments in the global risks landscape. The concept of trends was introduced in both the survey and the report and some of the global risks analysed in the past were relabelled and classified under a different category or better defined as trends.

The Global Risks Perception Survey (GRPS or survey) was adjusted accordingly to capture the main aspects of both risks and trends and to assess their interconnectedness and impact on societies. The following section describes the survey and methodology in greater detail.

The Global Risks Perception Survey

The Global Risks Perception Survey, discussed in Part 1, is the main instrument for assessing global risks and trends in this report. The survey was conducted between mid-July and the end of September 2014 among the World Economic Forum’s multistakeholder communities of leaders from business, government, academia and non-governmental and international organizations.¹

Raw responses were cleaned to improve overall data quality and completeness. All questionnaires with a completion rate of below 50% were dropped, reducing the number of available responses from 1,120 to 896.

In 12 cases, the respondent did not provide any information about gender, but it was possible to infer this information from the other records provided (first and last names). Similarly, 101 respondents did not indicate the region in which they are based and were manually assigned to one on the basis of their country of residence. Among the respondents, 43% completed the survey last year. Details of the sample composition are reported in Figure B.1.

The graph below shows the profile of the 896 survey respondents. To capture the voice of youth, the survey also targeted the World Economic Forum’s community of Global Shapers.² Those under 30 years of age accounted for approximately one-fifth of respondents.

Figure B.1: The Global Risks Perception Survey Sample Composition

Note: Reported shares are based on number of valid responses: Gender: 895 responses; Expertise: 883; Organization type: 885; Age distribution: 882; Region: 847.
The Global Risks Landscape 2015 (Figure 1)

Respondents were asked to assess the likelihood and global impact of each of the 28 risks. For each risk, they were asked, “How likely is this risk to occur globally within the next 10 years?” and “What is the estimated impact globally if this risk were to materialize? (Impact is to be interpreted in a broad sense beyond just economic consequences).” The possible answers ranged from 1 (“very unlikely” and “low” impact, respectively) to 7 (“very likely” and “high” impact, respectively). Respondents were given the possibility to choose a “Don’t know” option if they felt unable to provide an informed answer. For each risk, partial responses, i.e., those assessing only the likelihood or only the impact, were dropped. A simple average for both likelihood and impact for each of the 28 global risks was calculated on this basis. Formally, for any given risk $i$, its likelihood and impact, denoted as likelihood$_i,n$ and impact$_i,n$, respectively are:

$$\text{likelihood}_i,n = \frac{1}{N} \sum_{n=1}^{N} \text{likelihood}_{i,n}$$

$$\text{impact}_i,n = \frac{1}{N} \sum_{n=1}^{N} \text{impact}_{i,n}$$

where likelihood$_i,n$ and impact$_i,n$ are respectively the likelihood and impact assigned by respondent $n$ to risk $i$ and measured on a scale from 1 to 7. $N$ is the number of respondents for risk $i$ who assessed both the likelihood and impact of that risk.

The Global Risks and Risks-Trends Interconnections Maps (Figures 2 and 3)

To draw the global risks interconnections map presented in Part 1, survey respondents were asked to answer the following question: “In your view, which are the most strongly connected risks? Please select at least three pairs and up to six pairs from the 13 trends below (you can select the same trend and risk more than once).” The information thus obtained was used to construct the risks-trends interconnections map included in the inside cover flaps of the report.

In both cases, a tally was made of the number of times each pair was cited. To obtain normalized connection weights, this value was divided by the count of the most frequently cited pair and, in addition, this ratio was square-rooted to dampen the long-tail effect (i.e., a few very strong links, and many weak ones) for display and presentation purposes. Of the 378 possible pairs of risks, 122, or 32%, were not cited. Similarly, of the possible 364 trend-risk combinations, 116, or 32%, were not cited. Formally, the intensity of the interconnection between risks $i$ and $j$ (or between trend $i$ and risk $j$), denoted as interconnection$_{ij}$, corresponds to:

$$\text{interconnection}_{ij} = \frac{\text{pair}_{ij,n}}{\text{pair}_{\text{max}}}$$

where $N$ is the number of respondents. Variable pair$_{ij,n}$ is 1 when respondent $n$ selected the pair of risks $i$ and $j$ as part of his/her selection. Otherwise, it is 0. The value of the interconnection determines the thickness and brightness of each connecting line in the graph, with the most frequently cited pair having the thickest and brightest line.

In the global risks and risks-trends interconnections maps (Figures 2 and 3), the area of each node (corresponding to a risk or a trend) is scaled according to the number of times the corresponding risk or trend was cited as a part of the connection pair.

The placement of the nodes was computed using ForceAtlas2, a force-directed network layout algorithm implemented in Gephi software, which minimizes edge lengths and edge crossings by running a physical particle simulation.

The Risks of Highest Concern (Figure 1.1)

Although the report generally focuses on a time horizon of 10 years, respondents were asked to identify the risks of highest concern within two different time frames: 18 months and 10 years. To identify the top 10 global risks of highest concern, described in Part 1, respondents answered the following question: “In this survey, we are looking at risks within the next 10 years. For this question only, please select the five global risks that you believe to be of most concern within the next 18 months and 10 years, respectively.” For any given risk $i$ from the list of 28 risks, the share of total respondents ($N = 896$) that declared risk $i$ as a risk of concern and 0 otherwise. The risks with the 10 highest shares were selected as the risks of most concern.

Progress and Preparedness (Figure 1.7 and Figure 3.1)

Survey respondents were asked to identify up to three risks for which they felt most progress to address them has been made over the past 10 years. Similarly, they were asked to select up to three risks which they believed their region was least prepared for.

For any given risk $i$ from the list of 28 risks, the share of total respondents ($N = 896$) who thought that their region is least prepared was obtained:

$$\% \text{ progress}_i = \frac{1}{N} \sum_{n=1}^{N} \text{p}_{i,n}$$

with $p_{i,n}$ equal to 1 if respondent $N$ selected risk $i$, and 0 otherwise.

Similarly, the share of total respondents who thought that their region is least prepared for risk $i$ was obtained:

$$\% \text{ preparedness}_i = \frac{1}{N} \sum_{n=1}^{N} r_{i,n}$$

with $r_{i,n}$ equal to 1 if respondent $N$ selected risk $i$, and 0 otherwise.
Appendix C: The Executive Opinion Survey and Views of the Business Community on the Impact of Global Risks on Their Business

Every year since 1979, the World Economic Forum conducts the Executive Opinion Survey (EOS). This survey captures invaluable information on a broad range of socio-economic issues. In the 2014 edition, over 13,000 executives in 144 economies were surveyed. The 2014 edition of the EOS, conducted between February and May 2014, for the first time included a question on the risks of biggest concern. More specifically, respondents were asked to select the five global risks that they were most concerned about for doing business in their country and to rank these five risks from 1 (for the one of highest concern) to 5 (for the one of lowest concern).

This list of 19 global risks (Table C.1) in the EOS is different from that used in the present report, although a majority of risks on the former list do appear on the latter, albeit slightly reformulated in some cases. The EOS list was established before the Global Risks Perceptions Survey (GRPS) methodology was reviewed and a number of risks were redefined or excluded and others were introduced. In addition, whereas the GRPS was agnostic about the impact of global risks on a particular group, the EOS question specifically asked about the impact on the ability to do business in the respondent’s country. Furthermore, the EOS did not specify any time horizon, unlike the GRPS which considered a 10-year horizon. Finally, the size and nature of the two samples of respondents differed significantly: a multistakeholder group of experts in the case of the GRPS and business executives in the case of the EOS.

For these reasons, the results of the GRPS and EOS are not strictly comparable. Instead, the EOS results provide a complementary perspective – that of businesses on the impact of global risks on their businesses.

To rank the 19 risks based on the level of concern, each received a score derived from the rank assigned by respondents, from 5 for the risk the respondent ranked first, to 1 for the risk ranked fifth (all non-cited risks were assigned a score of zero). As a second step, for each economy the sum of points obtained by each risk across all responses from that economy was divided by the total of points distributed across all risks in the economy. The risk score thus obtained was used to establish a country-level ranking.

Figure C.1: Global Risks of Highest Concern for Doing Business, Per Country

Note: Only risks that are of highest concern in at least two countries are represented on the map. Other risks of highest concern: Violent interstate conflict (in Armenia), Breakdown of critical information infrastructure and networks (Cameroon), Escalation of economic and resource nationalism (Lesotho), and Greater incidence of environmentally-related events (Philippines).
Figure C.2 reports the results at the global level, as well as for the two main development status groups, advanced economies and emerging market and developing economies. Aggregate scores correspond to the average scores of each risk across all economies belonging to the group of interest.

Figure C.1 shows a snapshot of the data on a map. Based on the results, fiscal crises is the risk of highest concern for doing business in 93 (65%) of the 144 economies covered by the survey, well ahead of oil price shock and profound political and social instability, both of which come first in 13 economies (9%). The map in Figure C.1 is shaded according to the risk of highest concern. Within a troubled geopolitical context, a fragile and uneven recovery in advanced economies, and a slowdown in many emerging economies, it is not surprising that economic risks are those of most immediate and highest concern to businesses.

In advanced economies, concerns about economic risks are even higher. Fiscal crises is the risk of highest concern in 30 of the 35 advanced economies. In Austria, Germany and Switzerland, failure of a major financial mechanism or institution is the one of highest concern, whereas liquidity crises is the risk of top concern in Portugal and Spain.

Among emerging market and developing economies, fiscal crises is the risk of highest concern – by far – but oil price shock comes second, followed by liquidity crises. Prolonged neglect of critical infrastructure ranks fourth; a major obstacle to business development, economic integration and trade performance, it is the main concern in Côte d’Ivoire, Mozambique, Paraguay and Uganda.

Interested readers can visit the Global Risks report’s portal at www.weforum.org/risks to access the results for individual economies and regions.

### Table C.1: The Executive Opinion Survey 2014 List of 19 Global Risks

<table>
<thead>
<tr>
<th>Risk</th>
<th>All respondents</th>
<th>Advanced economies</th>
<th>Emerging market and developing economies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fiscal crises in key economies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure of a major financial mechanism or institution</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Liquidity crises</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oil price shock to the global economy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prolonged neglect of critical infrastructure and its development needs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Greater incidence of environmentally related events (weather, natural catastrophes, man-made catastrophes)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Water crises</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure of climate-change mitigation and adaptation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Major escalation in organized crime and illicit trade</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large-scale terrorist attacks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Violent interstate conflict with regional consequences</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Escalation of economic and resource nationalization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Food crises</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pandemic outbreak</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Profound political and social instability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breakdown of critical information infrastructure and networks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Escalation in large-scale cyber attacks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Massive incident of data fraud/theft</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mismanaged urbanization</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* denotes risks included in both the Global Risks Perception Survey and the Executive Opinion Survey
** denotes risks whose definition was redefined for the Global Risks Perception Survey 2014


### Figure C.2: Global Risks of Highest Concern for Doing Business, for Advanced Economies and Emerging Market and Developing Economies


Note: From the list of global risks above, respondents were asked to select the five global risks of highest concern for doing business in their country and to rank them between 1 (most problematic) and 5. The bars in the figure show the responses weighted according to their rankings.
Endnotes

1 See http://www.weforum.org/communities
2 The Global Shapers Community is a network of hubs developed and led by young people who are exceptional in their potential, achievement and drive to make a contribution to their communities. See http://www.weforum.org/community/global-shapers.
3 See Jacomy et al., 2012.
4 Respondents could select the region they were based in from the following list: Europe, Central Asia including Russia, East Asia and Pacific, South Asia, Sub-Saharan Africa, Middle-East and North Africa, Latin America and the Caribbean, North America, and Oceania.
5 For more information about the Survey, see Browne et al. 2014.
6 By construction in each economy, the sum of risk scores is therefore 100.
7 Development status classification is from the International Monetary Fund (situation as of April 2014).

References


The *Global Risks 2015* report synthesizes the insights, ideas and contributions of many individuals through workshops, group calls and research. The World Economic Forum and the Global Risks 2015 report team is grateful to all who took part in the challenge to think hard about global risks. Without their dedication, guidance and support, it would not have been possible to develop this report.

The World Economic Forum would like to thank our Strategic Partners Marsh & McLennan Companies and Zurich Insurance Group for their guidance, input and support. We also thank our academic advisers, the National University of Singapore, the Oxford Martin School at the University of Oxford and the Wharton Risk Management and Decision Processes Center at the University of Pennsylvania.

The *Global Risks 2015* report governance is represented by the Steering Board, the Advisory Board and the Activation Board, all of which have provided invaluable input and guidance.

**The Steering Board** includes:

John Drzik, President, Global Risk and Specialties, Marsh, United States  
Espen Barth Eide, Managing Director and Member of the Managing Board, World Economic Forum, Switzerland  
Axel Lehmann, Group Chief Risk Officer, Zurich Insurance Group, Switzerland

**The Advisory Board** is composed of:

Rolf Alter, Director, Public Governance and Territorial Development, Organisation for Economic Co-operation and Development (OECD), Paris  
Mario Blejer, Vice-Chairman, Banco Hipotecario, Argentina  
Oliver Chen, Head, Credit Modeling, Global Valuation, United Kingdom; Representing the National University of Singapore on the Advisory Board  
Megan Clark, Chief Executive Officer,
Global Risks 2015

Riccardo Moretto, Zurich Insurance Group, Switzerland
Gregory Renand, Zurich Insurance Group, Switzerland
Stephen Szaraz, Marsh & McLennan Companies, United States

Global Risks 2015 Report Corporate Partners (not already listed above)

Marsh & McLennan Companies (Marsh, Oliver Wyman)
Shaun Lu
Maurits Paling
Mark Pollard
Maurizio Quintavalle
Thomas M. Quigley
Nick Studer
Alex Wittenberg

Zurich Insurance Group
Daniel Eherer
John Scott

Global Risks 2015 Report Academic Advisers

National University of Singapore
Tan Chorh Chuan
Ho Teck Hua

Oxford Martin School, University of Oxford
Ian Goldin

Wharton Risk Management and Decision Processes Center, University of Pennsylvania
Howard Kunreuther

The project team would like to thank the following individuals for their contribution to the report:

Box 1.1: Global Risks team, World Economic Forum
Box 1.2: Dan Smith, International Alert
Box 1.3: Nouriel Roubini, New York University
Box 1.4: Jonathan Ostry, International Monetary Fund
Box 1.5: Erwann Michel-Kerjan and Howard Kunreuther, The Wharton School, University of Pennsylvania
Box 1.6: Bernice Lee, World Economic Forum

Box 1.7: Danil Kerimi, World Economic Forum
Box 1.2: Pascal Lamy, Notre Europe – Jacques Delors Institute
Box 2.2: Anja Kaspersen, World Economic Forum and Mark Leonard, European Council on Foreign Relations (ECFR)
Box 2.3: Anthony Townsend, New York University
Box 2.4: Arnaud Bernaert and Vanessa Candeias, World Economic Forum
Box 2.5: Caroline Galvan, World Economic Forum
Box 2.6: Anders Sandberg, University of Oxford
Box 2.7: Marie-Valentine Florin, International Risk Governance Council
Box 2.8: Bernhard Petermeier, World Economic Forum

The project team would like to thank the individuals who contributed to the report by participating in the workshop on the new methodology of the Global Risks 2015 report. In addition, the project team is grateful to the individuals who took part in the interviews and group calls conducted throughout the year for their valuable inputs.

The participants in the workshop on the methodology of the Global Risks 2015 report were:

Christoph Bleiker, ABB; Natalie Day, University of Sussex; Michael Furrer, Holcim; Evgeni Ivanitsov, European Risk Management Council; Randolph Kent, King’s College London; Nicholas Mueller, Swiss Federal Chancellery; Richard Stoffelen, Holcim; William Sutherland, University of Cambridge; Chadia Wannous, UN System Influenza Coordination (UNSIC), UNDP.
The individuals who took part in the interviews and group calls were:
Nayef Al-Rodhan, University of Oxford; Ian Anthony, Stockholm International Peace Research Institute; John Beard, World Health Organization; Adam Blackwell, Organization of American States; Antoine Bommier, Swiss Federal Institute of Technology (ETH) Risk Center; William Boulding, Duke University; Ian Bremmer, Eurasia Group; Milan Ćirković, University of Novi Sad; Belisario Contreras, Organization of American States (OAS); Mike Douglass, National University of Singapore; Carlos Gaiter, Circle of Blue; Donald Hanna, Roubini Global Economics; Ghassan Hasbani, Graycoats; Göran Hultin, Caden Corporation; Vincenzo Iozzo, Trail of Bits; Eugene Kaspersky, Kaspersky Lab; Michael Keith, University of Oxford; Felipe Larraín Bascuñán, Pontificia Universidad Catolica de Chile; Robert Lawrence, Harvard University; Lee Sang Yup, Korea Advanced Institute of Science and Technology (KAIST); Mark Leonard, European Council on Foreign Relations (ECFR); Li Tie, China Center for Urban Development; Masse Lo, Greenpeace; Maleeha Lodhi, Jang Group of Newspapers; Herbert M’cleod, Office of the President of Sierra Leone; Nicholas Mueller, Swiss Federal Chancellery; Mike Muller, National Planning Commission; Suzanne Nora Johnson, Brookings Institution; S. Jay Olshansky, University of Illinois; Rodrigo Pérez Mackenna, Ministry of Housing and Urban Development of Chile; Abhilash Panda, United Nations Office for Disaster Risk Reduction (UNISDR); Qian Qiyu, Nanyang Technological University; Guha Ramasubramanian, Wipro; Martin Rees, University of Cambridge; Ortwin Renn, University of Stuttgart; Stuart Russell, University of California, Berkeley; Razeen Sally, National University of Singapore; Dennis Snower, Kiel Institute for the World Economy; Shoji Takenaka, Toshiba Corporation; Coen Teulings, University of Amsterdam; Siddharth Tiwari, International Monetary Fund (IMF); Anthony Townsend, New York University; Dmitri Trenin, Carnegie Moscow Center; Adair Turner, Institute for New Economic Thinking (INET); and Stephen Walt, Harvard Kennedy School of Government.

The project team would like to thank the Members of the Global Agenda Council on Risk & Resilience and the Global Agenda Council on Geoeconomics for their contribution.

Global Agenda Council on Risk & Resilience: Valerie Amos, United Nations; Lauren Alexander Augustine, National Academy of Sciences; Stanley M. Bergman, Henry Schein; Michael Berkowitz, Rockefeller Foundation; Machariai Edwin, Dalberg Global Development Advisers; Victor Meyer, Deutsche Bank; Kjerstin Nielsen, Homeland Security Policy Institute; Satoru Nishikawa, Japan Water Agency (JWA); Yuichi Ono, Tohoku University; Sara Pantuliano, Overseas Development Institute; Joe Ruiz, The UPS Foundation; Armen Sarkissian, Eurasia House International; Shi Peijun, Beijing Normal University (BNU); Dan Smith, International Alert; Elizabeth Hauser Strand, Build Change; Jaan Tallinn, Centre for the Study of Existential Risk; Michael Useem, Wharton School; Margareta Wahlström, United Nations International Strategy for Disaster Reduction; Nick Wildgoose, Zurich Insurance Group; Alexander Wolfson, Citi.

Global Agenda Council on Geoeconomics: Sanjaya Baru, International Institute for Strategic Studies (IISS); Karan Bhatia, General Electric Company; Ian Bremmer, Eurasia Group; Michael Fullilove, Lowy Institute for International Policy; Nik Gowing, BBC World News; Sergei Guriev, Fondation Nationale des Sciences Politiques (Sciences Po); Victor Halberstadt, Leiden University; Parag Khanna, New America Foundation; Hina Rabbani Khar; Felipe Larraín Bascuñán, Pontificia Universidad Catolica de Chile; Paul A. Laudicina, A.T. Kearney; Mark Leonard, European Council on Foreign Relations (ECFR); Michael Levi, Council on Foreign Relations; Kishore Mahbubani, Lee Kuan Yew School of Public Policy, National University of Singapore; Takashi Mitachi, The Boston Consulting Group; Linah K. Mohohlo, Bank of Botswana; Moisés Naim, Carnegie Endowment for International Peace; Pan Wei, Peking University; Volker Perthes, Stiftung Wissenschaft und Politik (SWP); Douglas A. Rediker, Peterson Institute for International Economics; Ghassan Salamé, Paris School of International Affairs (PSIA), Institut d’Etudes Politiques; Dmitri Trenin, Carnegie Moscow Center; Yulia Tseplyaeva, Sberbank; Wu Xinbo, Fudan University.

At the World Economic Forum
Founder and Executive Chairman
Klaus Schwab

Management Committee

The Global Risks 2015 report Project Team
Margareta Drzeniek Hanouz, Lead Economist, Director; Ciara Browne, Director; Attilio Di Battista, Junior Quantitative Economist; Gaëlle Dreyer, Project Associate; Caroline Galvan, Economist, Senior Manager; Thierry Geiger, Economist, Associate Director; and Tania Gutknecht, Community Manager.

The Global Competitiveness and Risks Team
Roberto Crotti, Quantitative Economist, Manager; and Cecilia Serin, Senior Associate.

The Global Risks 2015 report Public Engagement Team
Oliver Cann, Director; and Amélie Weinzierl, Media Relations Associate

Production Team
Ann Brady, Associate Director; David Bustamante, Senior Manager; Marta Chierego, Associate Director; Kamal Kimaoui, Director; Fabienne Stassen, Freelance Editor; Moritz Stefaner, Freelance Information Visualizer; and Andrew Wright, Freelance Writer.
The project team expresses its gratitude to the colleagues from the World Economic Forum who provided advice and feedback throughout the development of the Global Risks 2015 report:

The World Economic Forum is an international institution committed to improving the state of the world through public-private cooperation in the spirit of global citizenship. It engages with business, political, academic and other leaders of society to shape global, regional and industry agendas.

Incorporated as a not-for-profit foundation in 1971 and headquartered in Geneva, Switzerland, the Forum is independent, impartial and not tied to any interests. It cooperates closely with all leading international organizations.
FEDERAL REGISTER

Vol. 78 Tuesday,
No. 33 February 19, 2013

Part III

The President

Executive Order 13636—Improving Critical Infrastructure Cybersecurity
Executive Order 13636 of February 12, 2013

Improving Critical Infrastructure Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation’s critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

Sec. 2. Critical Infrastructure. As used in this order, the term critical infrastructure means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Sec. 3. Policy Coordination. Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive–1 of February 13, 2009 (Organization of the National Security Council System), or any successor.

Sec. 4. Cybersecurity Information Sharing. (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the “Secretary”), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

(c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with 6 U.S.C. 143 and in collaboration with the Secretary of
Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.

(e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

Sec. 5. Privacy and Civil Liberties Protections. (a) Agencies shall coordinate their activities under this order with their senior agency officials for privacy and civil liberties and ensure that privacy and civil liberties protections are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency’s activities.

(b) The Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security (DHS) shall assess the privacy and civil liberties risks of the functions and programs undertaken by DHS as called for in this order and shall recommend to the Secretary ways to minimize or mitigate such risks, in a publicly available report, to be released within 1 year of the date of this order. Senior agency privacy and civil liberties officials for other agencies engaged in activities under this order shall conduct assessments of their agency activities and provide those assessments to DHS for consideration and inclusion in the report. The report shall be reviewed on an annual basis and revised as necessary. The report may contain a classified annex if necessary. Assessments shall include evaluation of activities against the Fair Information Practice Principles and other applicable privacy and civil liberties policies, principles, and frameworks. Agencies shall consider the assessments and recommendations of the report in implementing privacy and civil liberties protections for agency activities.

(c) In producing the report required under subsection (b) of this section, the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of DHS shall consult with the Privacy and Civil Liberties Oversight Board and coordinate with the Office of Management and Budget (OMB).

(d) Information submitted voluntarily in accordance with 6 U.S.C. 133 by private entities under this order shall be protected from disclosure to the fullest extent permitted by law.

Sec. 6. Consultative Process. The Secretary shall establish a consultative process to coordinate improvements to the cybersecurity of critical infrastructure. As part of the consultative process, the Secretary shall engage and consider the advice, on matters set forth in this order, of the Critical Infrastructure Partnership Advisory Council; Sector Coordinating Councils; critical infrastructure owners and operators; Sector-Specific Agencies; other relevant agencies; independent regulatory agencies; State, local, territorial, and tribal governments; universities; and outside experts.

Sec. 7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure. (a) The Secretary of Commerce shall direct the Director of the National
Institute of Standards and Technology (the “Director”) to lead the development of a framework to reduce cyber risks to critical infrastructure (the “Cybersecurity Framework”). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113), and OMB Circular A–119, as revised.

(b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

(d) In developing the Cybersecurity Framework, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, the National Security Agency, Sector-Specific Agencies and other interested agencies including OMB, owners and operators of critical infrastructure, and other stakeholders through the consultative process established in section 6 of this order. The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information and technical expertise to inform the development of the Cybersecurity Framework. The Secretary shall provide performance goals for the Cybersecurity Framework informed by work under section 9 of this order.

(e) Within 240 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework (the “preliminary Framework”). Within 1 year of the date of this order, and after coordination with the Secretary to ensure suitability under section 8 of this order, the Director shall publish a final version of the Cybersecurity Framework (the “final Framework”).

(f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, experience from the implementation of section 8 of this order, and any other relevant factors.

Sec. 8. Voluntary Critical Infrastructure Cybersecurity Program. (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the “Program”).
(b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

(c) Sector-Specific Agencies shall report annually to the President, through the Secretary, on the extent to which owners and operators notified under section 9 of this order are participating in the Program.

(d) The Secretary shall coordinate establishment of a set of incentives designed to promote participation in the Program. Within 120 days of the date of this order, the Secretary and the Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law and authorities to participants in the Program.

(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.

Sec. 9. Identification of Critical Infrastructure at Greatest Risk. (a) Within 150 days of the date of this order, the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in a catastrophic regional or national effects on public health or safety, economic security, or national security. In identifying critical infrastructure for this purpose, the Secretary shall use the consultative process established in section 6 of this order and draw upon the expertise of Sector-Specific Agencies. The Secretary shall apply consistent, objective criteria in identifying such critical infrastructure. The Secretary shall not identify any commercial information technology products or consumer information technology services under this section. The Secretary shall review and update the list of identified critical infrastructure under this section on an annual basis, and provide such lists to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs.

(b) Heads of Sector-Specific Agencies and other relevant agencies shall provide the Secretary with information necessary to carry out the responsibilities under this section. The Secretary shall develop a process for other relevant stakeholders to submit information to assist in making the identifications required in subsection (a) of this section.

(c) The Secretary, in coordination with Sector-Specific Agencies, shall confidentially notify owners and operators of critical infrastructure identified under subsection (a) of this section that they have been so identified, and ensure identified owners and operators are provided the basis for the determination. The Secretary shall establish a process through which owners and operators of critical infrastructure may submit relevant information and request reconsideration of identifications under subsection (a) of this section.

Sec. 10. Adoption of Framework. (a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification
of critical infrastructure required under section 9 of this order. Within 90
days of the publication of the preliminary Framework, these agencies shall
submit a report to the President, through the Assistant to the President
for Homeland Security and Counterterrorism, the Director of OMB, and
the Assistant to the President for Economic Affairs, that states whether
or not the agency has clear authority to establish requirements based upon
the Cybersecurity Framework to sufficiently address current and projected
cyber risks to critical infrastructure, the existing authorities identified, and
any additional authority required.

(b) If current regulatory requirements are deemed to be insufficient, within
90 days of publication of the final Framework, agencies identified in sub-
section (a) of this section shall propose prioritized, risk-based, efficient,
and coordinated actions, consistent with Executive Order 12866 of Septem-
ber 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January
18, 2011 (Improving Regulation and Regulatory Review), and Executive Order
13609 of May 1, 2012 (Promoting International Regulatory Cooperation),
to mitigate cyber risk.

(c) Within 2 years after publication of the final Framework, consistent
with Executive Order 13563 and Executive Order 13610 of May 10, 2012
(Identifying and Reducing Regulatory Burdens), agencies identified in sub-
section (a) of this section shall, in consultation with owners and operators
of critical infrastructure, report to OMB on any critical infrastructure subject
to ineffective, conflicting, or excessively burdensome cybersecurity require-
ments. This report shall describe efforts made by agencies, and make rec-
ommendations for further actions, to minimize or eliminate such require-
ments.

(d) The Secretary shall coordinate the provision of technical assistance
to agencies identified in subsection (a) of this section on the development
of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the
security of critical infrastructure are encouraged to engage in a consultative
process with the Secretary, relevant Sector-Specific Agencies, and other
affected parties to consider prioritized actions to mitigate cyber risks for
critical infrastructure consistent with their authorities.

Sec. 11. Definitions. (a) “Agency” means any authority of the United States
that is an “agency” under 44 U.S.C. 3502(1), other than those considered
to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) “Critical Infrastructure Partnership Advisory Council” means the coun-
cil established by DHS under 6 U.S.C. 451 to facilitate effective interaction
and coordination of critical infrastructure protection activities among the
Federal Government; the private sector; and State, local, territorial, and
tribal governments.

(c) “Fair Information Practice Principles” means the eight principles set
forth in Appendix A of the National Strategy for Trusted Identities in Cyber-
space.

(d) “Independent regulatory agency” has the meaning given the term in
44 U.S.C. 3502(5).

(e) “Sector Coordinating Council” means a private sector coordinating
council composed of representatives of owners and operators within a par-
ticular sector of critical infrastructure established by the National Infrastruc-
ture Protection Plan or any successor.

(f) “Sector-Specific Agency” has the meaning given the term in Presidential
Policy Directive–21 of February 12, 2013 (Critical Infrastructure Security
and Resilience), or any successor.

Sec. 12. General Provisions. (a) This order shall be implemented consistent
with applicable law and subject to the availability of appropriations. Nothing
in this order shall be construed to provide an agency with authority for
regulating the security of critical infrastructure in addition to or to a greater
extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.

(d) This order shall be implemented consistent with U.S. international obligations.

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

THE WHITE HOUSE,

February 12, 2013.

[FR Doc. 2013-03915
Filed 2-15-13; 11:15 am]
Billing code 3295-F3
PRESIDENTIAL POLICY DIRECTIVE/PPD-21

SUBJECT: Critical Infrastructure Security and Resilience

The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

Introduction

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being.

The Nation's critical infrastructure is diverse and complex. It includes distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations. Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient.

Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery.

This directive establishes national policy on critical infrastructure security and resilience. This endeavor is a shared responsibility among the Federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure (herein referred to as "critical infrastructure owners and operators"). This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the Federal Government, as well as enhances overall coordination and collaboration. The Federal Government also has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators.
Policy

It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats. The Federal Government shall work with critical infrastructure owners and operators and SLTT entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof. These efforts shall seek to reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure.

The Federal Government shall also engage with international partners to strengthen the security and resilience of domestic critical infrastructure and critical infrastructure located outside of the United States on which the Nation depends.

U.S. efforts shall address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect this infrastructure's interconnectedness and interdependency. This directive also identifies energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors.

Three strategic imperatives shall drive the Federal approach to strengthen critical infrastructure security and resilience:

1) Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience;
2) Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and
3) Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.

All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions. Such infrastructure shall be addressed in the plans and execution of the requirements in the National Continuity Policy.

Federal departments and agencies shall implement this directive in a manner consistent with applicable law, Presidential directives, and Federal regulations, including those protecting privacy, civil rights, and civil liberties. In addition, Federal departments and agencies shall protect all information associated with carrying out this directive consistent with applicable legal authorities and policies.

Roles and Responsibilities

Effective implementation of this directive requires a national unity of effort pursuant to strategic guidance from the Secretary of Homeland Security. That national effort must include expertise and day-to-day engagement from the Sector-Specific Agencies (SSAs) as well as the specialized or support capabilities from other Federal departments and agencies, and
strong collaboration with critical infrastructure owners and operators and SLTT entities. Although the roles and responsibilities identified in this directive are directed at Federal departments and agencies, effective partnerships with critical infrastructure owners and operators and SLTT entities are imperative to strengthen the security and resilience of the Nation's critical infrastructure.

Secretary of Homeland Security
The Secretary of Homeland Security shall provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure. In carrying out the responsibilities assigned in the Homeland Security Act of 2002, as amended, the Secretary of Homeland Security evaluates national capabilities, opportunities, and challenges in protecting critical infrastructure; analyzes threats to, vulnerabilities of, and potential consequences from all hazards on critical infrastructure; identifies security and resilience functions that are necessary for effective public-private engagement with all critical infrastructure sectors; develops a national plan and metrics, in coordination with SSAs and other critical infrastructure partners; integrates and coordinates Federal cross-sector security and resilience activities; identifies and analyzes key interdependencies among critical infrastructure sectors; and reports on the effectiveness of national efforts to strengthen the Nation's security and resilience posture for critical infrastructure.

Additional roles and responsibilities for the Secretary of Homeland Security include:

1) Identify and prioritize critical infrastructure, considering physical and cyber threats, vulnerabilities, and consequences, in coordination with SSAs and other Federal departments and agencies;

2) Maintain national critical infrastructure centers that shall provide a situational awareness capability that includes integrated, actionable information about emerging trends, imminent threats, and the status of incidents that may impact critical infrastructure;

3) In coordination with SSAs and other Federal departments and agencies, provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators and facilitate access to and exchange of information and intelligence necessary to strengthen the security and resilience of critical infrastructure;

4) Conduct comprehensive assessments of the vulnerabilities of the Nation's critical infrastructure in coordination with the SSAs and in collaboration with SLTT entities and critical infrastructure owners and operators;

5) Coordinate Federal Government responses to significant cyber or physical incidents affecting critical infrastructure consistent with statutory authorities;

6) Support the Attorney General and law enforcement agencies with their responsibilities to investigate and prosecute threats to and attacks against critical infrastructure;

7) Coordinate with and utilize the expertise of SSAs and other appropriate Federal departments and agencies to map geospatially, image, analyze, and sort critical infrastructure by employing commercial satellite and airborne systems, as well as existing capabilities within other departments and agencies; and
8) Report annually on the status of national critical infrastructure efforts as required by statute.

Sector-Specific Agencies
Each critical infrastructure sector has unique characteristics, operating models, and risk profiles that benefit from an identified Sector-Specific Agency that has institutional knowledge and specialized expertise about the sector. Recognizing existing statutory or regulatory authorities of specific Federal departments and agencies, and leveraging existing sector familiarity and relationships, SSAs shall carry out the following roles and responsibilities for their respective sectors:

1) As part of the broader national effort to strengthen the security and resilience of critical infrastructure, coordinate with the Department of Homeland Security (DHS) and other relevant Federal departments and agencies and collaborate with critical infrastructure owners and operators, where appropriate with independent regulatory agencies, and with SLTT entities, as appropriate, to implement this directive;

2) Serve as a day-to-day Federal interface for the dynamic prioritization and coordination of sector-specific activities;

3) Carry out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations;

4) Provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate; and

5) Support the Secretary of Homeland Security's statutorily required reporting requirements by providing an annual basis sector-specific critical infrastructure information.

Additional Federal Responsibilities
The following departments and agencies have specialized or support functions related to critical infrastructure security and resilience that shall be carried out by, or along with, other Federal departments and agencies and independent regulatory agencies, as appropriate.

1) The Department of State, in coordination with DHS, SSAs, and other Federal departments and agencies, shall engage foreign governments and international organizations to strengthen the security and resilience of critical infrastructure located outside the United States and to facilitate the overall exchange of best practices and lessons learned for promoting the security and resilience of critical infrastructure on which the Nation depends.

2) The Department of Justice (DOJ), including the Federal Bureau of Investigation (FBI), shall lead counterterrorism and counterintelligence investigations and related law enforcement activities across the critical infrastructure sectors. DOJ shall investigate, disrupt, prosecute, and otherwise reduce foreign intelligence, terrorist, and other threats to, and actual or attempted attacks on, or sabotage of, the Nation's critical infrastructure. The FBI also conducts domestic collection, analysis, and dissemination of cyber threat information, and shall be responsible for the operation of the National Cyber Investigative Joint Task Force (NCIJTF). The NCIJTF serves as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from DHS, the Intelligence Community (IC), the Department of
Defense (DOD), and other agencies as appropriate. The Attorney General and the Secretary of Homeland Security shall collaborate to carry out their respective critical infrastructure missions.

3) The Department of the Interior, in collaboration with the SSA for the Government Facilities Sector, shall identify, prioritize, and coordinate the security and resilience efforts for national monuments and icons and incorporate measures to reduce risk to these critical assets, while also promoting their use and enjoyment.

4) The Department of Commerce (DOC), in collaboration with DHS and other relevant Federal departments and agencies, shall engage private sector, research, academic, and government organizations to improve security for technology and tools related to cyber-based systems, and promote the development of other efforts related to critical infrastructure to enable the timely availability of industrial products, materials, and services to meet homeland security requirements.

5) The IC, led by the Director of National Intelligence (DNI), shall use applicable authorities and coordination mechanisms to provide, as appropriate, intelligence assessments regarding threats to critical infrastructure and coordinate on intelligence and other sensitive or proprietary information related to critical infrastructure. In addition, information security policies, directives, standards, and guidelines for safeguarding national security systems shall be overseen as directed by the President, applicable law, and in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

6) The General Services Administration, in consultation with DOD, DHS, and other departments and agencies as appropriate, shall provide or support government-wide contracts for critical infrastructure systems and ensure that such contracts include audit rights for the security and resilience of critical infrastructure.

7) The Nuclear Regulatory Commission (NRC) is to oversee its licensees' protection of commercial nuclear power reactors and non-power nuclear reactors used for research, testing, and training; nuclear materials in medical, industrial, and academic settings, and facilities that fabricate nuclear fuel; and the transportation, storage, and disposal of nuclear materials and waste. The NRC is to collaborate, to the extent possible, with DHS, DOJ, the Department of Energy, the Environmental Protection Agency, and other Federal departments and agencies, as appropriate, on strengthening critical infrastructure security and resilience.

8) The Federal Communications Commission, to the extent permitted by law, is to exercise its authority and expertise to partner with DHS and the Department of State, as well as other Federal departments and agencies and SSAs as appropriate, on: (1) identifying and prioritizing communications infrastructure; (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and (3) working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends.
9) Federal departments and agencies shall provide timely information to the Secretary of Homeland Security and the national critical infrastructure centers necessary to support cross-sector analysis and inform the situational awareness capability for critical infrastructure.

Three Strategic Imperatives

1) Refine and Clarify Functional Relationships across the Federal Government to Advance the National Unity of Effort to Strengthen Critical Infrastructure Security and Resilience

An effective national effort to strengthen critical infrastructure security and resilience must be guided by a national plan that identifies roles and responsibilities and is informed by the expertise, experience, capabilities, and responsibilities of the SSAs, other Federal departments and agencies with critical infrastructure roles, SLTT entities, and critical infrastructure owners and operators.

During the past decade, new programs and initiatives have been established to address specific infrastructure issues, and priorities have shifted and expanded. As a result, Federal functions related to critical infrastructure security and resilience shall be clarified and refined to establish baseline capabilities that will reflect this evolution of knowledge, to define relevant Federal program functions, and to facilitate collaboration and information exchange between and among the Federal Government, critical infrastructure owners and operators, and SLTT entities.

As part of this refined structure, there shall be two national critical infrastructure centers operated by DHS – one for physical infrastructure and another for cyber infrastructure. They shall function in an integrated manner and serve as focal points for critical infrastructure partners to obtain situational awareness and integrated, actionable information to protect the physical and cyber aspects of critical infrastructure. Just as the physical and cyber elements of critical infrastructure are inextricably linked, so are the vulnerabilities. Accordingly, an integration and analysis function (further developed in Strategic Imperative 3) shall be implemented between these two national centers.

The success of these national centers, including the integration and analysis function, is dependent on the quality and timeliness of the information and intelligence they receive from the SSAs and other Federal departments and agencies, as well as from critical infrastructure owners and operators and SLTT entities.

These national centers shall not impede the ability of the heads of Federal departments and agencies to carry out or perform their responsibilities for national defense, criminal, counterintelligence, counterterrorism, or investigative activities.

2) Enable Efficient Information Exchange by Identifying Baseline Data and Systems Requirements for the Federal Government

A secure, functioning, and resilient critical infrastructure requires the efficient exchange of information, including intelligence, between all levels of governments and critical
infrastructure owners and operators. This must facilitate the timely exchange of threat and vulnerability information as well as information that allows for the development of a situational awareness capability during incidents. The goal is to enable efficient information exchange through the identification of requirements for data and information formats and accessibility, system interoperability, and redundant systems and alternate capabilities should there be a disruption in the primary systems.

Greater information sharing within the government and with the private sector can and must be done while respecting privacy and civil liberties. Federal departments and agencies shall ensure that all existing privacy principles, policies, and procedures are implemented consistent with applicable law and policy and shall include senior agency officials for privacy in their efforts to govern and oversee information sharing properly.

3) Implement an Integration and Analysis Function to Inform Planning and Operational Decisions Regarding Critical Infrastructure

The third strategic imperative builds on the first two and calls for the implementation of an integration and analysis function for critical infrastructure that includes operational and strategic analysis on incidents, threats, and emerging risks. It shall reside at the intersection of the two national centers as identified in Strategic Imperative 1, and it shall include the capability to collate, assess, and integrate vulnerability and consequence information with threat streams and hazard information to:

a. Aid in prioritizing assets and managing risks to critical infrastructure;
b. Anticipate interdependencies and cascading impacts;
c. Recommend security and resilience measures for critical infrastructure prior to, during, and after an event or incident; and

d. Support incident management and restoration efforts related to critical infrastructure.

This function shall not replicate the analysis function of the IC or the National Counterterrorism Center, nor shall it involve intelligence collection activities. The IC, DOD, DOJ, DHS, and other Federal departments and agencies with relevant intelligence or information shall, however, inform this integration and analysis capability regarding the Nation's critical infrastructure by providing relevant, timely, and appropriate information to the national centers. This function shall also use information and intelligence provided by other critical infrastructure partners, including SLTT and nongovernmental analytic entities.

Finally, this integration and analysis function shall support DHS's ability to maintain and share, as a common Federal service, a near real-time situational awareness capability for critical infrastructure that includes actionable information about imminent threats, significant trends, and awareness of incidents that may affect critical infrastructure.

Innovation and Research and Development
The Secretary of Homeland Security, in coordination with the Office of Science and Technology Policy (OSTP), the SSAs, DOC, and other Federal departments and agencies, shall provide input to align those Federal and Federally-funded research and development (R&D) activities that seek to strengthen the security and resilience of the Nation's critical infrastructure, including:

1) Promoting R&D to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology;
2) Enhancing modeling capabilities to determine potential impacts on critical infrastructure of an incident or threat scenario, as well as cascading effects on other sectors;
3) Facilitating initiatives to incentivize cybersecurity investments and the adoption of critical infrastructure design features that strengthen all-hazards security and resilience; and
4) Prioritizing efforts to support the strategic guidance issued by the Secretary of Homeland Security.

**Implementation of the Directive**

The Secretary of Homeland Security shall take the following actions as part of the implementation of this directive.

1) **Critical Infrastructure Security and Resilience Functional Relationships.** Within 120 days of the date of this directive, the Secretary of Homeland Security shall develop a description of the functional relationships within DHS and across the Federal Government related to critical infrastructure security and resilience. It should include the roles and functions of the two national critical infrastructure centers and a discussion of the analysis and integration function. When complete, it should serve as a roadmap for critical infrastructure owners and operators and SLTT entities to navigate the Federal Government's functions and primary points of contact assigned to those functions for critical infrastructure security and resilience against both physical and cyber threats. The Secretary shall coordinate this effort with the SSAs and other relevant Federal departments and agencies. The Secretary shall provide the description to the President through the Assistant to the President for Homeland Security and Counterterrorism.

2) **Evaluation of the Existing Public-Private Partnership Model.** Within 150 days of the date of this directive, the Secretary of Homeland Security, in coordination with the SSAs, other relevant Federal departments and agencies, SLTT entities, and critical infrastructure owners and operators, shall conduct an analysis of the existing public-private partnership model and recommend options for improving the effectiveness of the partnership in both the physical and cyber space. The evaluation shall consider options to streamline processes for collaboration and exchange of information and to minimize duplication of effort. Furthermore, the analysis shall consider how the model can be flexible and adaptable to meet the unique needs of individual sectors while providing a focused, disciplined, and effective approach for the Federal Government to coordinate with the critical infrastructure owners and operators and with SLTT governments. The evaluation shall result in recommendations to enhance partnerships to be approved for implementation through the
processes established in the Organization of the National Security Council System directive.

3) **Identification of Baseline Data and Systems Requirements for the Federal Government to Enable Efficient Information Exchange.** Within 180 days of the date of this directive, the Secretary of Homeland Security, in coordination with the SSAs and other Federal departments and agencies, shall convene a team of experts to identify baseline data and systems requirements to enable the efficient exchange of information and intelligence relevant to strengthening the security and resilience of critical infrastructure. The experts should include representatives from those entities that routinely possess information important to critical infrastructure security and resilience; those that determine and manage information technology systems used to exchange information; and those responsible for the security of information being exchanged. Interoperability with critical infrastructure partners; identification of key data and the information requirements of key Federal, SLTT, and private sector entities; availability, accessibility, and formats of data; the ability to exchange various classifications of information; and the security of those systems to be used; and appropriate protections for individual privacy and civil liberties should be included in the analysis. The analysis should result in baseline requirements for sharing of data and interoperability of systems to enable the timely exchange of data and information to secure critical infrastructure and make it more resilient. The Secretary shall provide that analysis to the President through the Assistant to the President for Homeland Security and Counterterrorism.

4) **Development of a Situational Awareness Capability for Critical Infrastructure.** Within 240 days of the date of this directive, the Secretary of Homeland Security shall demonstrate a near real-time situational awareness capability for critical infrastructure that includes threat streams and all-hazards information as well as vulnerabilities; provides the status of critical infrastructure and potential cascading effects; supports decision making; and disseminates critical information that may be needed to save or sustain lives, mitigate damage, or reduce further degradation of a critical infrastructure capability throughout an incident. This capability should be available for and cover physical and cyber elements of critical infrastructure, and enable an integration of information as necessitated by the incident.

5) **Update to National Infrastructure Protection Plan.** Within 240 days of the date of this directive, the Secretary of Homeland Security shall provide to the President, through the Assistant to the President for Homeland Security and Counterterrorism, a successor to the National Infrastructure Protection Plan to address the implementation of this directive, the requirements of Title II of the Homeland Security Act of 2002 as amended, and alignment with the National Preparedness Goal and System required by PPD-8. The plan shall include the identification of a risk management framework to be used to strengthen the security and resilience of critical infrastructure; the methods to be used to prioritize critical infrastructure; the protocols to be used to synchronize communication and actions within the Federal Government; and a metrics and analysis process to be used to measure the Nation's ability to manage and reduce risks to
critical infrastructure. The updated plan shall also reflect the identified functional relationships within DHS and across the Federal Government and the updates to the public-private partnership model. Finally, the plan should consider sector dependencies on energy and communications systems, and identify pre-event and mitigation measures or alternate capabilities during disruptions to those systems. The Secretary shall coordinate this effort with the SSAs, other relevant Federal departments and agencies, SLTT entities, and critical infrastructure owners and operators.

6) National Critical Infrastructure Security and Resilience R&D Plan. Within 2 years of the date of this directive, the Secretary of Homeland Security, in coordination with the OSTP, the SSAs, DOC, and other Federal departments and agencies, shall provide to the President, through the Assistant to the President for Homeland Security and Counterterrorism, a National Critical Infrastructure Security and Resilience R&D Plan that takes into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide R&D requirements and investments. The plan should be issued every 4 years after its initial delivery, with interim updates as needed.

Policy coordination, dispute resolution, and periodic in-progress reviews for the implementation of this directive shall be carried out consistent with PPD-1, including the use of Interagency Policy Committees coordinated by the National Security Staff.

Nothing in this directive alters, supersedes, or impedes the authorities of Federal departments and agencies, including independent regulatory agencies, to carry out their functions and duties consistent with applicable legal authorities and other Presidential guidance and directives, including, but not limited to, the designation of critical infrastructure under such authorities.

This directive revokes Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, issued December 17, 2003. Plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded.

**Designated Critical Infrastructure Sectors and Sector-Specific Agencies**

This directive identifies 16 critical infrastructure sectors and designates associated Federal SSAs. In some cases co-SSAs are designated where those departments share the roles and responsibilities of the SSA. The Secretary of Homeland Security shall periodically evaluate the need for and approve changes to critical infrastructure sectors and shall consult with the Assistant to the President for Homeland Security and Counterterrorism before changing a critical infrastructure sector or a designated SSA for that sector. The sectors and SSAs are as follows:

**Chemical:**
Sector-Specific Agency: Department of Homeland Security

**Commercial Facilities:**
Sector-Specific Agency: Department of Homeland Security
Communications:
Sector-Specific Agency: Department of Homeland Security

Critical Manufacturing:
Sector-Specific Agency: Department of Homeland Security

Dams:
Sector-Specific Agency: Department of Homeland Security

Defense Industrial Base:
Sector-Specific Agency: Department of Defense

Emergency Services:
Sector-Specific Agency: Department of Homeland Security

Energy:
Sector-Specific Agency: Department of Energy

Financial Services:
Sector-Specific Agency: Department of the Treasury

Food and Agriculture:
Co-Sector-Specific Agencies: U.S. Department of Agriculture and Department of Health and Human Services

Government Facilities:
Co-Sector-Specific Agencies: Department of Homeland Security and General Services Administration

Healthcare and Public Health:
Sector-Specific Agency: Department of Health and Human Services

Information Technology:
Sector-Specific Agency: Department of Homeland Security

Nuclear Reactors, Materials, and Waste:
Sector-Specific Agency: Department of Homeland Security

Transportation Systems:
Co-Sector-Specific Agencies: Department of Homeland Security and Department of Transportation

Water and Wastewater Systems:
Sector-Specific Agency: Environmental Protection Agency

Definitions

For purposes of this directive:

The term "all hazards" means a threat or an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.

The term "collaboration" means the process of working together to achieve shared goals.
The terms "coordinate" and "in coordination with" mean a consensus decision-making process in which the named coordinating department or agency is responsible for working with the affected departments and agencies to achieve consensus and a consistent course of action.

The term "critical infrastructure" has the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

The term "Federal departments and agencies" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

The term "national essential functions" means that subset of Government functions that are necessary to lead and sustain the Nation during a catastrophic emergency.

The term "primary mission essential functions" means those Government functions that must be performed in order to support or implement the performance of the national essential functions before, during, and in the aftermath of an emergency.

The term "national security systems" has the meaning given to it in the Federal Information Security Management Act of 2002 (44 U.S.C. 3542(b)).

The term "resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

The term "Sector-Specific Agency" (SSA) means the Federal department or agency designated under this directive to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.

The terms "secure" and "security" refer to reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.

# # #
Table of Contents

Executive Summary .........................................................................................................................1
1.0 Framework Introduction .........................................................................................................3
2.0 Framework Basics ...................................................................................................................7
3.0 How to Use the Framework .................................................................................................13
Appendix A: Framework Core .....................................................................................................18
Appendix B: Glossary ....................................................................................................................37
Appendix C: Acronyms .................................................................................................................39

List of Figures

Figure 1: Framework Core Structure .............................................................................................. 7
Figure 2: Notional Information and Decision Flows within an Organization ................................. 12

List of Tables

Table 1: Function and Category Unique Identifiers ..................................................................... 19
Table 2: Framework Core ............................................................................................................. 20
Executive Summary

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation’s security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company’s bottom line. It can drive up costs and impact revenue. It can harm an organization’s ability to innovate and to gain and maintain customers.

To better address these risks, the President issued Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” on February 12, 2013, which established that “[i]t is the Policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.” In enacting this policy, the Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes. The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.

The Executive Order also requires that the Framework include a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities. While processes and existing needs will differ, the Framework can assist organizations in incorporating privacy and civil liberties as part of a comprehensive cybersecurity program.

The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The Framework provides organization and structure to today’s multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can also be
used by organizations located outside the United States and can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

Use of this voluntary Framework is the next step to improve the cybersecurity of our Nation’s critical infrastructure – providing guidance for individual organizations, while increasing the cybersecurity posture of the Nation’s critical infrastructure as a whole.
1.0 Framework Introduction

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. To strengthen the resilience of this infrastructure, President Obama issued Executive Order 13636 (EO), “Improving Critical Infrastructure Cybersecurity,” on February 12, 2013. This Executive Order calls for the development of a voluntary Cybersecurity Framework (“Framework”) that provides a “prioritized, flexible, repeatable, performance-based, and cost-effective approach” to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services. The Framework, developed in collaboration with industry, provides guidance to an organization on managing cybersecurity risk.

Critical infrastructure is defined in the EO as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” Due to the increasing pressures from external and internal threats, organizations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk. This approach is necessary regardless of an organization’s size, threat exposure, or cybersecurity sophistication today.

The critical infrastructure community includes public and private owners and operators, and other entities with a role in securing the Nation’s infrastructure. Members of each critical infrastructure sector perform functions that are supported by information technology (IT) and industrial control systems (ICS). This reliance on technology, communication, and the interconnectivity of IT and ICS has changed and expanded the potential vulnerabilities and increased potential risk to operations. For example, as ICS and the data produced in ICS operations are increasingly used to deliver critical services and support business decisions, the potential impacts of a cybersecurity incident on an organization’s business, assets, health and safety of individuals, and the environment should be considered. To manage cybersecurity risks, a clear understanding of the organization’s business drivers and security considerations specific to its use of IT and ICS is required. Because each organization’s risk is unique, along with its use of IT and ICS, the tools and methods used to achieve the outcomes described by the Framework will vary.

Recognizing the role that the protection of privacy and civil liberties plays in creating greater public trust, the Executive Order requires that the Framework include a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities. Many organizations already have processes for addressing privacy and civil liberties. The methodology is designed to complement such processes and provide guidance to facilitate privacy risk management consistent with an organization’s approach to cybersecurity risk management. Integrating privacy and cybersecurity can benefit organizations by increasing customer confidence, enabling more standardized sharing of information, and simplifying operations across legal regimes.

---

To ensure extensibility and enable technical innovation, the Framework is technology neutral. The Framework relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience. By relying on those global standards, guidelines, and practices developed, managed, and updated by industry, the tools and methods available to achieve the Framework outcomes will scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements. The use of existing and emerging standards will enable economies of scale and drive the development of effective products, services, and practices that meet identified market needs. Market competition also promotes faster diffusion of these technologies and practices and realization of many benefits by the stakeholders in these sectors.

Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:

1) Describe their current cybersecurity posture;
2) Describe their target state for cybersecurity;
3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4) Assess progress toward the target state;
5) Communicate among internal and external stakeholders about cybersecurity risk.

The Framework complements, and does not replace, an organization’s risk management process and cybersecurity program. The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.

Just as the Framework is not industry-specific, the common taxonomy of standards, guidelines, and practices that it provides also is not country-specific. Organizations outside the United States may also use the Framework to strengthen their own cybersecurity efforts, and the Framework can contribute to developing a common language for international cooperation on critical infrastructure cybersecurity.

1.1 Overview of the Framework

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities. These components are explained below.

- The **Framework Core** is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization’s management of cybersecurity risk. The Framework Core
then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

- **Framework Implementation Tiers** ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization’s cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization’s practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

- A **Framework Profile** ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a “Current” Profile (the “as is” state) with a “Target” Profile (the “to be” state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization’s risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

### 1.2 Risk Management and the Cybersecurity Framework

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance.

With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.

The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes. Thus, the Framework gives organizations the ability to dynamically select and direct improvement in cybersecurity risk management for the IT and ICS environments.

1.3 Document Overview

The remainder of this document contains the following sections and appendices:

- **Section 2** describes the Framework components: the Framework Core, the Tiers, and the Profiles.
- **Section 3** presents examples of how the Framework can be used.
- **Appendix A** presents the Framework Core in a tabular format: the Functions, Categories, Subcategories, and Informative References.
- **Appendix B** contains a glossary of selected terms.
- **Appendix C** lists acronyms used in this document.
2.0 Framework Basics

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization. Different types of entities – including sector coordinating structures, associations, and organizations – can use the Framework for different purposes, including the creation of common Profiles.

2.1 Framework Core

The Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by industry as helpful in managing cybersecurity risk. The Core comprises four elements: Functions, Categories, Subcategories, and Informative References, depicted in Figure 1:

<table>
<thead>
<tr>
<th>Functions</th>
<th>Categories</th>
<th>Subcategories</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROTECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DETECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RESPOND</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECOVER</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 1: Framework Core Structure

The Framework Core elements work together as follows:

- **Functions** organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.

- **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Access Control,” and “Detection Processes.”
Subcategories further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”

Informative References are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process.

The five Framework Core Functions are defined below. These Functions are not intended to form a serial path, or lead to a static desired end state. Rather, the Functions can be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk. See Appendix A for the complete Framework Core listing.

- Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

  The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

- Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

  The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

- Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

  The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

- Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

---

7 NIST developed a Compendium of informative references gathered from the Request for Information (RFI) input, Cybersecurity Framework workshops, and stakeholder engagement during the Framework development process. The Compendium includes standards, guidelines, and practices to assist with implementation. The Compendium is not intended to be an exhaustive list, but rather a starting point based on initial stakeholder input. The Compendium and other supporting material can be found at http://www.nist.gov/cyberframework/.
The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

### 2.2 Framework Implementation Tiers

The Framework Implementation Tiers (“Tiers”) provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor and sophistication in cybersecurity risk management practices and the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization’s overall risk management practices. Risk management considerations include many aspects of cybersecurity, including the degree to which privacy and civil liberties considerations are integrated into an organization’s management of cybersecurity risk and potential risk responses.

The Tier selection process considers an organization’s current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. Organizations should determine the desired Tier, ensuring that the selected level meets the organizational goals, is feasible to implement, and reduces cybersecurity risk to critical assets and resources to levels acceptable to the organization. Organizations should consider leveraging external guidance obtained from Federal government departments and agencies, Information Sharing and Analysis Centers (ISACs), existing maturity models, or other sources to assist in determining their desired tier.

While organizations identified as Tier 1 (Partial) are encouraged to consider moving toward Tier 2 or greater, Tiers do not represent maturity levels. Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective. Successful implementation of the Framework is based upon achievement of the outcomes described in the organization’s Target Profile(s) and not upon Tier determination.
The Tier definitions are as follows:

**Tier 1: Partial**

- **Risk Management Process** – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.

- **Integrated Risk Management Program** – There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.

- **External Participation** – An organization may not have the processes in place to participate in coordination or collaboration with other entities.

**Tier 2: Risk Informed**

- **Risk Management Process** – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.

- **Integrated Risk Management Program** – There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis.

- **External Participation** – The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.

**Tier 3: Repeatable**

- **Risk Management Process** – The organization’s risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.

- **Integrated Risk Management Program** – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.

- **External Participation** – The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.
Tier 4: Adaptive

- **Risk Management Process** – The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.

- **Integrated Risk Management Program** – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.

- **External Participation** – The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

### 2.3 Framework Profile

The Framework Profile ("Profile") is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs.

Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. Profiles support business/mission requirements and aid in the communication of risk within and between organizations. This Framework document does not prescribe Profile templates, allowing for flexibility in implementation.

Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be addressed to meet cybersecurity risk management objectives. An action plan to address these gaps can contribute to the roadmap described above. Prioritization of gap mitigation is driven by the organization’s business needs and risk management processes. This risk-based approach enables an organization to gauge resource estimates (e.g., staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner.
2.4 Coordination of Framework Implementation

Figure 2 describes a common flow of information and decisions at the following levels within an organization:

- Executive
- Business/Process
- Implementation/Operations

The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into the risk management process, and then collaborates with the implementation/operations level to communicate business needs and create a Profile. The implementation/operations level communicates the Profile implementation progress to the business/process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization’s overall risk management process and to the implementation/operations level for awareness of business impact.
3.0 How to Use the Framework

An organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Utilizing the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program. The Framework provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization’s cybersecurity practices. It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program.

The following sections present different ways in which organizations can use the Framework.

3.1 Basic Review of Cybersecurity Practices

The Framework can be used to compare an organization’s current cybersecurity activities with those outlined in the Framework Core. Through the creation of a Current Profile, organizations can examine the extent to which they are achieving the outcomes described in the Core Categories and Subcategories, aligned with the five high-level Functions: Identify, Protect, Detect, Respond, and Recover. An organization may find that it is already achieving the desired outcomes, thus managing cybersecurity commensurate with the known risk. Conversely, an organization may determine that it has opportunities to (or needs to) improve. The organization can use that information to develop an action plan to strengthen existing cybersecurity practices and reduce cybersecurity risk. An organization may also find that it is overinvesting to achieve certain outcomes. The organization can use this information to reprioritize resources to strengthen other cybersecurity practices.

While they do not replace a risk management process, these five high-level Functions will provide a concise way for senior executives and others to distill the fundamental concepts of cybersecurity risk so that they can assess how identified risks are managed, and how their organization stacks up at a high level against existing cybersecurity standards, guidelines, and practices. The Framework can also help an organization answer fundamental questions, including “How are we doing?” Then they can move in a more informed way to strengthen their cybersecurity practices where and when deemed necessary.

3.2 Establishing or Improving a Cybersecurity Program

The following steps illustrate how an organization could use the Framework to create a new cybersecurity program or improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity.
Step 1: Prioritize and Scope. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance.

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization’s overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations seek to incorporate emerging risks and threat and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization’s desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next it creates a prioritized action plan to address those gaps that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The organization then determines resources necessary to address the gaps. Using Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take in regards to the gaps, if any, identified in the previous step. It then monitors its current cybersecurity practices against the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

An organization may repeat the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the orient
step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also utilize this process to align their cybersecurity program with their desired Framework Implementation Tier.

3.3 Communicating Cybersecurity Requirements with Stakeholders
The Framework provides a common language to communicate requirements among interdependent stakeholders responsible for the delivery of essential critical infrastructure services. Examples include:

- An organization may utilize a Target Profile to express cybersecurity risk management requirements to an external service provider (e.g., a cloud provider to which it is exporting data).
- An organization may express its cybersecurity state through a Current Profile to report results or to compare with acquisition requirements.
- A critical infrastructure owner/operator, having identified an external partner on whom that infrastructure depends, may use a Target Profile to convey required Categories and Subcategories.
- A critical infrastructure sector may establish a Target Profile that can be used among its constituents as an initial baseline Profile to build their tailored Target Profiles.

3.4 Identifying Opportunities for New or Revised Informative References
The Framework can be used to identify opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging needs. An organization implementing a given Subcategory, or developing a new Subcategory, might discover that there are few Informative References, if any, for a related activity. To address that need, the organization might collaborate with technology leaders and/or standards bodies to draft, develop, and coordinate standards, guidelines, or practices.

3.5 Methodology to Protect Privacy and Civil Liberties
This section describes a methodology as required by the Executive Order to address individual privacy and civil liberties implications that may result from cybersecurity operations. This methodology is intended to be a general set of considerations and processes since privacy and civil liberties implications may differ by sector or over time and organizations may address these considerations and processes with a range of technical implementations. Nonetheless, not all activities in a cybersecurity program may give rise to these considerations. Consistent with Section 3.4, technical privacy standards, guidelines, and additional best practices may need to be developed to support improved technical implementations.

Privacy and civil liberties implications may arise when personal information is used, collected, processed, maintained, or disclosed in connection with an organization’s cybersecurity activities. Some examples of activities that bear privacy or civil liberties considerations may include: cybersecurity activities that result in the over-collection or over-retention of personal information; disclosure or use of personal information unrelated to cybersecurity activities; cybersecurity mitigation activities that result in denial of service or other similar potentially
adverse impacts, including activities such as some types of incident detection or monitoring that may impact freedom of expression or association.

The government and agents of the government have a direct responsibility to protect civil liberties arising from cybersecurity activities. As referenced in the methodology below, government or agents of the government that own or operate critical infrastructure should have a process in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements.

To address privacy implications, organizations may consider how, in circumstances where such measures are appropriate, their cybersecurity program might incorporate privacy principles such as: data minimization in the collection, disclosure, and retention of personal information material related to the cybersecurity incident; use limitations outside of cybersecurity activities on any information collected specifically for cybersecurity activities; transparency for certain cybersecurity activities; individual consent and redress for adverse impacts arising from use of personal information in cybersecurity activities; data quality, integrity, and security; and accountability and auditing.

As organizations assess the Framework Core in Appendix A, the following processes and activities may be considered as a means to address the above-referenced privacy and civil liberties implications:

**Governance of cybersecurity risk**

- An organization’s assessment of cybersecurity risk and potential risk responses considers the privacy implications of its cybersecurity program
- Individuals with cybersecurity-related privacy responsibilities report to appropriate management and are appropriately trained
- Process is in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements
- Process is in place to assess implementation of the foregoing organizational measures and controls

**Approaches to identifying and authorizing individuals to access organizational assets and systems**

- Steps are taken to identify and address the privacy implications of access control measures to the extent that they involve collection, disclosure, or use of personal information

**Awareness and training measures**

- Applicable information from organizational privacy policies is included in cybersecurity workforce training and awareness activities
- Service providers that provide cybersecurity-related services for the organization are informed about the organization’s applicable privacy policies
Anomalous activity detection and system and assets monitoring

- Process is in place to conduct a privacy review of an organization’s anomalous activity detection and cybersecurity monitoring

Response activities, including information sharing or other mitigation efforts

- Process is in place to assess and address whether, when, how, and the extent to which personal information is shared outside the organization as part of cybersecurity information sharing activities
- Process is in place to conduct a privacy review of an organization’s cybersecurity mitigation efforts
Appendix A: Framework Core

This appendix presents the Framework Core: a listing of Functions, Categories, Subcategories, and Informative References that describe specific cybersecurity activities that are common across all critical infrastructure sectors. The chosen presentation format for the Framework Core does not suggest a specific implementation order or imply a degree of importance of the Categories, Subcategories, and Informative References. The Framework Core presented in this appendix represents a common set of activities for managing cybersecurity risk. While the Framework is not exhaustive, it is extensible, allowing organizations, sectors, and other entities to use Subcategories and Informative References that are cost-effective and efficient and that enable them to manage their cybersecurity risk. Activities can be selected from the Framework Core during the Profile creation process and additional Categories, Subcategories, and Informative References may be added to the Profile. An organization’s risk management processes, legal/regulatory requirements, business/mission objectives, and organizational constraints guide the selection of these activities during Profile creation. Personal information is considered a component of data or assets referenced in the Categories when assessing security risks and protections.

While the intended outcomes identified in the Functions, Categories, and Subcategories are the same for IT and ICS, the operational environments and considerations for IT and ICS differ. ICS have a direct effect on the physical world, including potential risks to the health and safety of individuals, and impact on the environment. Additionally, ICS have unique performance and reliability requirements compared with IT, and the goals of safety and efficiency must be considered when implementing cybersecurity measures.

For ease of use, each component of the Framework Core is given a unique identifier. Functions and Categories each have a unique alphabetic identifier, as shown in Table 1. Subcategories within each Category are referenced numerically; the unique identifier for each Subcategory is included in Table 2.

Additional supporting material relating to the Framework can be found on the NIST website at http://www.nist.gov/cyberframework/.
<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td><strong>IDENTIFY</strong> (ID)</td>
<td><strong>(ID)</strong></td>
<td><strong>Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.</strong></td>
<td></td>
</tr>
</tbody>
</table>
| | | **ID.AM-1:** Physical devices and systems within the organization are inventoried | • CCS CSC 1  
• COBIT 5 BA109.01, BA109.02  
• ISA 62443-2-1:2009 4.2.3.4  
• ISA 62443-3-3:2013 SR 7.8  
• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2  
• NIST SP 800-53 Rev. 4 CM-8 |
| | | **ID.AM-2:** Software platforms and applications within the organization are inventoried | • CCS CSC 2  
• COBIT 5 BA109.01, BA109.02, BA109.05  
• ISA 62443-2-1:2009 4.2.3.4  
• ISA 62443-3-3:2013 SR 7.8  
• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2  
• NIST SP 800-53 Rev. 4 CM-8 |
| | | **ID.AM-3:** Organizational communication and data flows are mapped | • CCS CSC 2  
• COBIT 5 DSS05.02  
• ISA 62443-2-1:2009 4.2.3.4  
• ISO/IEC 27001:2013 A.13.2.1  
• NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 |
| | | **ID.AM-4:** External information systems are catalogued | • COBIT 5 APO02.02  
• ISO/IEC 27001:2013 A.11.2.6  
• NIST SP 800-53 Rev. 4 AC-20, SA-9 |
| | | **ID.AM-5:** Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value | • COBIT 5 APO03.03, APO03.04, BA109.02  
• ISA 62443-2-1:2009 4.2.3.6  
• ISO/IEC 27001:2013 A.8.2.1  
• NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 |
| | | **ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | • COBIT 5 APO01.02, DSS06.03  
• ISA 62443-2-1:2009 4.3.2.3.3  
• ISO/IEC 27001:2013 A.6.1.1 |
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| **Business Environment (ID.BE):**  
The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. | ID.BE-1: The organization’s role in the supply chain is identified and communicated | - NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 |
| | ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated | - COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05  
- ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2  
- NIST SP 800-53 Rev. 4 CP-2, SA-12 |
| | ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated | - COBIT 5 APO02.06, APO03.01  
- NIST SP 800-53 Rev. 4 PM-8 |
| | ID.BE-4: Dependencies and critical functions for delivery of critical services are established | - ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3  
- NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14 |
| | ID.BE-5: Resilience requirements to support delivery of critical services are established | - COBIT 5 DSS04.02  
- NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14 |
| **Governance (ID.GV):**  
The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. | ID.GV-1: Organizational information security policy is established | - COBIT 5 APO01.03, EDM01.01, EDM01.02  
- ISA 62443-2-1:2009 4.3.2.6  
- ISO/IEC 27001:2013 A.5.1.1  
- NIST SP 800-53 Rev. 4 -1 controls from all families |
| | ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners | - COBIT 5 APO13.12  
- ISA 62443-2-1:2009 4.3.2.3  
- ISO/IEC 27001:2013 A.6.1.1, A.7.2.1  
- NIST SP 800-53 Rev. 4 PM-1, PS-7 |
| | ID.GV-3: Legal and regulatory requirements regarding cybersecurity, | - COBIT 5 MEA03.01, MEA03.04  
- ISA 62443-2-1:2009 4.4.3.7 |
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
|          |          | including privacy and civil liberties obligations, are understood and managed | • ISO/IEC 27001:2013 A.18.1  
• NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1) |
| ID.GV-4: | Governance and risk management processes address cybersecurity risks | • COBIT 5 DSS04.02  
• ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3  
• NIST SP 800-53 Rev. 4 PM-9, PM-11 |
| ID.RA-1: | Asset vulnerabilities are identified and documented | • CCS CSC 4  
• COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04  
• ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12  
• ISO/IEC 27001:2013 A.12.6.1, A.18.2.3  
• NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 |
| ID.RA-2: | Threat and vulnerability information is received from information sharing forums and sources | • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12  
• ISO/IEC 27001:2013 A.6.1.4  
• NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5 |
| ID.RA-3: | Threats, both internal and external, are identified and documented | • COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04  
• ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12  
• NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16 |
| ID.RA-4: | Potential business impacts and likelihoods are identified | • COBIT 5 DSS04.02  
• ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12  
• NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14 |
| ID.RA-5: | Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | • COBIT 5 APO12.02  
• ISO/IEC 27001:2013 A.12.6.1  
• NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16 |
| ID.RA-6: | Risk responses are identified and | • COBIT 5 APO12.05, APO13.02 |

**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PROTECT (PR)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Risk Management Strategy (ID.RM):</strong> The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</td>
<td>• NIST SP 800-53 Rev. 4 PM-4, PM-9</td>
</tr>
</tbody>
</table>
|            |          | **ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders | • COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02  
• ISA 62443-2-1:2009 4.3.4.2  
• NIST SP 800-53 Rev. 4 PM-9 |
|            |          | **ID.RM-2:** Organizational risk tolerance is determined and clearly expressed | • COBIT 5 APO12.06  
• ISA 62443-2-1:2009 4.3.2.6.5  
• NIST SP 800-53 Rev. 4 PM-9 |
|            |          | **ID.RM-3:** The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | • NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14 |
|            |          | **Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. | • CCS CSC 16  
• COBIT 5 DSS05.04, DSS06.03  
• ISA 62443-2-1:2009 4.3.3.5.1  
• ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9  
• NIST SP 800-53 Rev. 4 AC-2, IA Family |
|            |          | **PR.AC-1:** Identities and credentials are managed for authorized devices and users | • COBIT 5 DSS01.04, DSS05.05  
• ISA 62443-2-1:2009 4.3.3.2, 4.3.3.3.8  
• NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 |
|            |          | **PR.AC-2:** Physical access to assets is managed and protected               | • COBIT 5 APO13.01, DSS01.04, DSS05.03  
• ISA 62443-2-1:2009 4.3.3.6.6  
• ISA 62443-3-3:2013 SR 1.13, SR 2.6  
<p>|            |          | <strong>PR.AC-3:</strong> Remote access is managed                                        |                                                                                                                                                    |</p>
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties</td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20</td>
<td></td>
</tr>
</tbody>
</table>
| PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate | | • CCS CSC 12, 15  
• ISA 62443-2-1:2009 4.3.3.7.3  
• ISA 62443-3-3:2013 SR 2.1  
• NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16 |
| PR.AT-1: All users are informed and trained | | • CCS CSC 9  
• COBIT 5 APO07.03, BAI05.07  
• ISA 62443-2-1:2009 4.3.2.4.2  
• ISO/IEC 27001:2013 A.7.2.2  
• NIST SP 800-53 Rev. 4 AT-2, PM-13 |
| PR.AT-2: Privileged users understand roles & responsibilities | | • CCS CSC 9  
• COBIT 5 APO07.02, DSS06.03  
• ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3  
• ISO/IEC 27001:2013 A.6.1.1, A.7.2.2  
• NIST SP 800-53 Rev. 4 AT-3, PM-13 |
| PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities | | • CCS CSC 9  
• COBIT 5 APO07.03, APO10.04, APO10.05  
• ISA 62443-2-1:2009 4.3.2.4.2  
• ISO/IEC 27001:2013 A.6.1.1, A.7.2.2  
• NIST SP 800-53 Rev. 4 PS-7, SA-9 |
| PR.AT-4: Senior executives understand roles & responsibilities | | • CCS CSC 9  
• COBIT 5 APO07.03 |
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| **PR.AT-5**: Physical and information security personnel understand roles & responsibilities | | | • ISA 62443-2-1:2009 4.3.2.4.2  
• ISO/IEC 27001:2013 A.6.1.1, A.7.2.2,  
• NIST SP 800-53 Rev. 4 AT-3, PM-13 |
| **PR.DS-1**: Data-at-rest is protected | | | • CCS CSC 9  
• COBIT 5 APO07.03  
• ISA 62443-2-1:2009 4.3.2.4.2  
• ISO/IEC 27001:2013 A.6.1.1, A.7.2.2,  
• NIST SP 800-53 Rev. 4 AT-3, PM-13 |
| **PR.DS-2**: Data-in-transit is protected | | | • CCS CSC 17  
• COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06  
• ISA 62443-3-3:2013 SR 3.4, SR 4.1  
• ISO/IEC 27001:2013 A.8.2.3  
• NIST SP 800-53 Rev. 4 SC-28 |
| **PR.DS-3**: Assets are formally managed throughout removal, transfers, and disposition | | | • COBIT 5 BAI09.03  
• ISA 62443-2-1:2009 4.4.3.3.3.9, 4.3.4.4.1  
• ISA 62443-3-3:2013 SR 4.2  
• ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7  
• NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16 |
| **PR.DS-4**: Adequate capacity to ensure availability is maintained | | | • COBIT 5 APO13.01  
• ISA 62443-3-3:2013 SR 7.1, SR 7.2  
• ISO/IEC 27001:2013 A.12.3.1 |

*Data Security (PR.DS):* Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR.DS-5:</td>
<td></td>
<td>Protections against data leaks are implemented</td>
<td>• NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• CCS CSC 17</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• COBIT 5 APO01.06</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-3-3:2013 SR 5.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4</td>
</tr>
<tr>
<td>PR.DS-6:</td>
<td></td>
<td>Integrity checking mechanisms are used to verify software, firmware, and information integrity</td>
<td>• ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 SI-7</td>
</tr>
<tr>
<td>PR.DS-7:</td>
<td></td>
<td>The development and testing environment(s) are separate from the production environment</td>
<td>• COBIT 5 BAI07.04</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISO/IEC 27001:2013 A.12.1.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 CM-2</td>
</tr>
</tbody>
</table>

**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

<p>| PR.IP-1:          |                | A baseline configuration of information technology/industrial control systems is created and maintained | • CCS CSC 3, 10                                                                                                                                         |
|                   |                |                                                                             | • COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05                                                                                                       |
|                   |                |                                                                             | • ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3                                                                                                                |
|                   |                |                                                                             | • ISA 62443-3-3:2013 SR 7.6                                                                                                                               |
|                   |                |                                                                             | • NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10                                                                                 |
| PR.IP-2:          |                | A System Development Life Cycle to manage systems is implemented            | • COBIT 5 APO13.01                                                                                                                                         |
|                   |                |                                                                             | • ISA 62443-2-1:2009 4.3.4.3.3                                                                                                                               |</p>
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR.IP-3:</td>
<td>Configuration change control</td>
<td>• NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>processes are in place</td>
<td>• COBIT 5 BAI06.01, BAI01.06</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ISA 62443-3-3:2013 SR 7.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR.IP-4:</td>
<td>Backups of information are conducted, maintained, and tested periodically</td>
<td>• COBIT 5 APO13.01</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ISA 62443-2-1:2009 4.3.4.3.9</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ISA 62443-3-3:2013 SR 7.3, SR 7.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR.IP-5:</td>
<td>Policy and regulations regarding the physical operating environment for organizational assets are met</td>
<td>• COBIT 5 DSS01.04, DSS05.05</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ISA 62443-3-3:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR.IP-6:</td>
<td>Data is destroyed according to policy</td>
<td>• COBIT 5 BAI09.03</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ISA 62443-2-1:2009 4.3.4.4.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ISA 62443-3-3:2013 SR 4.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NIST SP 800-53 Rev. 4 MP-6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR.IP-7:</td>
<td>Protection processes are continuously improved</td>
<td>• COBIT 5 APO11.06, DSS04.05</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Subcategory</td>
<td>Informative References</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
</tbody>
</table>
| PR.IP-8: | Effectiveness of protection technologies is shared with appropriate parties | • ISO/IEC 27001:2013 A.16.1.6  
• NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4 |
| PR.IP-9: | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed | • COBIT 5 DSS04.03  
• ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1  
• ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2  
• NIST SP 800-53 Rev. 4 CP-2, IR-8 |
| PR.IP-10: | Response and recovery plans are tested | • ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11  
• ISA 62443-3-3:2013 SR 3.3  
• ISO/IEC 27001:2013 A.17.1.3  
• NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14 |
| PR.IP-11: | Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | • COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05  
• ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3  
• ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4  
• NIST SP 800-53 Rev. 4 PS Family |
| PR.IP-12: | A vulnerability management plan is developed and implemented | • ISO/IEC 27001:2013 A.12.6.1, A.18.2.2  
• NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2 |

**Maintenance (PR.MA):**

Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| PR.MA-1: | Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | • COBIT 5 BAI09.03  
• ISA 62443-2-1:2009 4.3.3.3.7  
• ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5  
• NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5 |
| PR.MA-2: | Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | • COBIT 5 DSS05.04  
• ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8  
• ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 |
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protectiv Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 MA-4</td>
</tr>
<tr>
<td>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</td>
<td></td>
<td></td>
<td>CCS CSC 14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 APO11.04</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 AU Family</td>
</tr>
<tr>
<td>PR.PT-2: Removable media is protected and its use restricted according to policy</td>
<td></td>
<td></td>
<td>COBIT 5 DSS05.02, APO13.01</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-3-3:2013 SR 2.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7</td>
</tr>
<tr>
<td>PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality</td>
<td></td>
<td></td>
<td>COBIT 5 DSS05.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ISO/IEC 27001:2013 A.9.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NIST SP 800-53 Rev. 4 AC-3, CM-7</td>
</tr>
<tr>
<td>PR.PT-4: Communications and control networks are protected</td>
<td></td>
<td></td>
<td>CCS CSC 7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COBIT 5 DSS05.02, APO13.01</td>
</tr>
</tbody>
</table>
| | | | ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1,
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| DETECT (DE) | Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood. | DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed | SR 7.6  
• ISO/IEC 27001:2013 A.13.1.1, A.13.2.1  
• NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7 |
| | | DE.AE-2: Detected events are analyzed to understand attack targets and methods | • COBIT 5 DSS03.01  
• ISA 62443-2-1:2009 4.4.3.3  
• NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4 |
| | | DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors | • ISA 62443-3-3:2013 SR 6.1  
• NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 |
| | | DE.AE-4: Impact of events is determined | • COBIT 5 APO12.06  
• NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4 |
| | | DE.AE-5: Incident alert thresholds are established | • COBIT 5 APO12.06  
• ISA 62443-2-1:2009 4.2.3.10  
• NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8 |
| Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. | DE.CM-1: The network is monitored to detect potential cybersecurity events | • CCS CSC 14, 16  
• COBIT 5 DSS05.07  
• ISA 62443-3-3:2013 SR 6.2  
• NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 |
<p>| | | DE.CM-2: The physical environment is | • ISA 62443-2-1:2009 4.3.3.3.8 |</p>
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitored to detect potential cybersecurity events</td>
<td>DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events</td>
<td>• NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20</td>
<td></td>
</tr>
<tr>
<td>DE.CM-4: Malicious code is detected</td>
<td>• ISA 62443-3-3:2013 SR 6.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ISO/IEC 27001:2013 A.12.4.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE.CM-5: Unauthorized mobile code is detected</td>
<td>• ISA 62443-3-3:2013 SR 2.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ISO/IEC 27001:2013 A.12.5.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events</td>
<td>• COBIT 5 APO07.06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ISO/IEC 27001:2013 A.14.2.7, A.15.2.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed</td>
<td>• NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE.CM-8: Vulnerability scans are performed</td>
<td>• COBIT 5 BA103.10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ISO/IEC 27001:2013 A.12.6.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• NIST SP 800-53 Rev. 4 RA-5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Detection Processes (DE.DP):**
Detection processes and procedures are maintained and tested to ensure timely and accountability

<p>| DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability | • CCS CSC 5 |
| • COBIT 5 DSS05.01 |
| • ISA 62443-2-1:2009 4.4.3.1 |
| • ISO/IEC 27001:2013 A.6.1.1 |</p>
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>adequate awareness of anomalous events.</td>
<td>• NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14</td>
</tr>
</tbody>
</table>
| **DE.DP-2:** Detection activities comply with all applicable requirements |          |             | • ISA 62443-2-1:2009 4.4.3.2  
• ISO/IEC 27001:2013 A.18.1.4  
• NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4 |
| **DE.DP-3:** Detection processes are tested |          |             | • COBIT 5 APO13.02  
• ISA 62443-2-1:2009 4.4.3.2  
• ISA 62443-3-3:2013 SR 3.3  
• ISO/IEC 27001:2013 A.14.2.8  
• NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 |
| **DE.DP-4:** Event detection information is communicated to appropriate parties |          |             | • COBIT 5 APO12.06  
• ISA 62443-2-1:2009 4.3.4.5.9  
• ISA 62443-3-3:2013 SR 6.1  
• ISO/IEC 27001:2013 A.16.1.2  
• NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4 |
| **DE.DP-5:** Detection processes are continuously improved |          |             | • COBIT 5 APO11.06, DSS04.05  
• ISA 62443-2-1:2009 4.4.3.4  
• ISO/IEC 27001:2013 A.16.1.6  
• NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 |
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| **RESPOND (RS)** | **Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events. | **RS.RP-1:** Response plan is executed during or after an event | • COBIT 5 BA101.10  
• CCS CSC 18  
• ISA 62443-2-1:2009 4.3.4.5.1  
• ISO/IEC 27001:2013 A.16.1.5  
• NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8 |
| **Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. | **RS.CO-1:** Personnel know their roles and order of operations when a response is needed | • ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4  
• ISO/IEC 27001:2013 A.6.1.1, A.16.1.1  
• NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8 |
|  | **RS.CO-2:** Events are reported consistent with established criteria | • ISA 62443-2-1:2009 4.3.4.5.5  
• NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8 |
|  | **RS.CO-3:** Information is shared consistent with response plans | • ISA 62443-2-1:2009 4.3.4.5.2  
• ISO/IEC 27001:2013 A.16.1.2  
• NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 |
|  | **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans | • ISA 62443-2-1:2009 4.3.4.5.5  
• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 |
|  | **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | • NIST SP 800-53 Rev. 4 PM-15, SI-5 |
| **Analysis (RS.AN):** Analysis is conducted to ensure adequate response and support recovery activities. | **RS.AN-1:** Notifications from detection systems are investigated | • COBIT 5 DSS02.07  
• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8  
• ISA 62443-3-3:2013 SR 6.1  
• ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5  
• NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
</table>
| RS.AN-2: The impact of the incident is understood | • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8  
• ISO/IEC 27001:2013 A.16.1.6  
• NIST SP 800-53 Rev. 4 CP-2, IR-4 |
| RS.AN-3: Forensics are performed | • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1  
• ISO/IEC 27001:2013 A.16.1.7  
• NIST SP 800-53 Rev. 4 AU-7, IR-4 |
| RS.AN-4: Incidents are categorized consistent with response plans | • ISA 62443-2-1:2009 4.3.4.5.6  
• ISO/IEC 27001:2013 A.16.1.4  
• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8 |

**Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

| RS.MI-1: Incidents are contained | • ISA 62443-2-1:2009 4.3.4.5.6  
• ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4  
• ISO/IEC 27001:2013 A.16.1.5  
• NIST SP 800-53 Rev. 4 IR-4 |
| RS.MI-2: Incidents are mitigated | • ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10  
• ISO/IEC 27001:2013 A.12.2.1, A.16.1.5  
• NIST SP 800-53 Rev. 4 IR-4 |
| RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks | • ISO/IEC 27001:2013 A.12.6.1  
• NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5 |

**Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

| RS.IM-1: Response plans incorporate lessons learned | • COBIT 5 BA101.13  
• ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4  
• ISO/IEC 27001:2013 A.16.1.6  
• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 |
| RS.IM-2: Response strategies are updated | • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 |

**RECOVER (RC)**

**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely recovery.

| RC.RP-1: Recovery plan is executed during or after an event | • CCS CSC 8  
• COBIT 5 DSS02.05, DSS03.04  
• ISO/IEC 27001:2013 A.16.1.5 |
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restoration of systems or assets affected by cybersecurity events.</strong></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8</td>
</tr>
<tr>
<td><strong>Improvements (RC.IM):</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery planning and processes are improved by incorporating lessons learned into future activities.</td>
<td>RC.IM-1: Recovery plans incorporate lessons learned</td>
<td>• COBIT 5 BA105.07</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ISA 62443-2-1:2009 4.4.3.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.IM-2: Recovery strategies are updated</td>
<td>• COBIT 5 BA107.08</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8</td>
</tr>
<tr>
<td><strong>Communications (RC.CO):</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.</td>
<td>RC.CO-1: Public relations are managed</td>
<td>• COBIT 5 EDM03.02</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO-2: Reputation after an event is repaired</td>
<td>• COBIT 5 MEA03.02</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams</td>
<td>• NIST SP 800-53 Rev. 4 CP-2, IR-4</td>
</tr>
</tbody>
</table>

Information regarding Informative References described in Appendix A may be found at the following locations:

- Control Objectives for Information and Related Technology (COBIT): [http://www.isaca.org/COBIT/Pages/default.aspx](http://www.isaca.org/COBIT/Pages/default.aspx)
Mappings between the Framework Core Subcategories and the specified sections in the Informative References represent a general correspondence and are not intended to definitively determine whether the specified sections in the Informative References provide the desired Subcategory outcome.
## Appendix B: Glossary

This appendix defines selected terms used in the publication.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
<td>The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Access Control,” and “Detection Processes.”</td>
</tr>
<tr>
<td><strong>Critical Infrastructure</strong></td>
<td>Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.</td>
</tr>
<tr>
<td><strong>Cybersecurity</strong></td>
<td>The process of protecting information by preventing, detecting, and responding to attacks.</td>
</tr>
<tr>
<td><strong>Cybersecurity Event</strong></td>
<td>A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).</td>
</tr>
<tr>
<td><strong>Detect (function)</strong></td>
<td>Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.</td>
</tr>
<tr>
<td><strong>Framework</strong></td>
<td>A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the “Cybersecurity Framework.”</td>
</tr>
<tr>
<td><strong>Framework Core</strong></td>
<td>A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.</td>
</tr>
<tr>
<td><strong>Framework Implementation Tier</strong></td>
<td>A lens through which to view the characteristics of an organization’s approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.</td>
</tr>
<tr>
<td><strong>Framework Profile</strong></td>
<td>A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.</td>
</tr>
<tr>
<td><strong>Function</strong></td>
<td>One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify,</td>
</tr>
</tbody>
</table>
Protect, Detect, Respond, and Recover.

**Identify (function)**
Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

**Informative Reference**
A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory.

**Mobile Code**
A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.

**Protect (function)**
Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

**Privileged User**
A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

**Recover (function)**
Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

**Respond (function)**
Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

**Risk**
A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

**Risk Management**
The process of identifying, assessing, and responding to risk.

**Subcategory**
The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”
Appendix C: Acronyms

This appendix defines selected acronyms used in the publication.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCS</td>
<td>Council on CyberSecurity</td>
</tr>
<tr>
<td>COBIT</td>
<td>Control Objectives for Information and Related Technology</td>
</tr>
<tr>
<td>DCS</td>
<td>Distributed Control System</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>EO</td>
<td>Executive Order</td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control Systems</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IR</td>
<td>Interagency Report</td>
</tr>
<tr>
<td>ISA</td>
<td>International Society of Automation</td>
</tr>
<tr>
<td>ISAC</td>
<td>Information Sharing and Analysis Center</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>RFI</td>
<td>Request for Information</td>
</tr>
<tr>
<td>RMP</td>
<td>Risk Management Process</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SP</td>
<td>Special Publication</td>
</tr>
</tbody>
</table>
About the Critical Infrastructure Cyber Community C³ Voluntary Program

The United States depends on critical infrastructure every day to provide energy, water, transportation, financial services, and other capabilities that support our needs and way of life. Over the years, improvements in technology have allowed these capabilities to evolve and run more efficiently.

With this increased reliance on cyber-dependent systems, some increased threats and vulnerabilities. Protecting the cybersecurity of our critical infrastructure is a top priority for the nation, and in February 2013 the President signed Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity and released Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience, which aims to increase the overall resilience of U.S. critical infrastructure. One of the major components of the EO is the development of the Cybersecurity Framework (the Framework) by the National Institute of Standards and Technology (NIST) to help critical infrastructure sectors and organizations reduce and manage their cyber risk.

Because cybersecurity and physical security are increasingly interconnected, the Department of Homeland Security (DHS) has partnered with the critical infrastructure community to establish a voluntary program to encourage use of the Framework to strengthen critical infrastructure cybersecurity. The Critical Infrastructure Cyber Community C³ (pronounced “C Cubed”) Voluntary Program is the coordination point within the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes. The C³ Voluntary Program aims to: 1) support industry in increasing its cyber resilience; 2) increase awareness and use of the Framework; and 3) encourage organizations to manage cybersecurity as part of an all hazards approach to enterprise risk management.

The C³ Voluntary Program’s launch in February 2014 coincides with the release of the final Framework. The C³ Voluntary Program’s focus during the first year will be engagement with Sector-Specific Agencies (SSAs) and organizations using the Framework to develop guidance on how to implement the Framework. Later phases of the C³ Voluntary Program will broaden the program’s reach to all critical infrastructure and businesses of all sizes that are interested in using the Framework.

C³ Voluntary Program Activities

The C³ Voluntary Program focuses on three major activities:

Supporting Use

The C³ Voluntary Program will assist stakeholders with understanding use of the Framework and other cyber risk management efforts, and support development of general and sector-specific guidance for Framework implementation. The C³ Voluntary Program will also work with the 16 critical infrastructure sectors to develop sector-specific guidance, as needed, for using the Framework.

Outreach and Communications

The C³ Voluntary Program will serve as a point of contact and customer relationship manager to assist organizations with Framework use, and guide interested organizations and sectors to DHS and other public and private sector resources to support use of the Cybersecurity Framework.

Feedback

The C³ Voluntary Program encourages feedback from stakeholder organizations about their experience using C³ Voluntary Program resources to implement the Framework. The C³ Voluntary Program works with organizations to understand how they are using the Framework, and to receive feedback on how the Framework and the C³ Voluntary Program can be improved to better serve organizations. Feedback about the Framework will also be shared with NIST, to help guide the development of the next version of the Framework and similar efforts.

**C³ Voluntary Program Engagement Channels**

The C³ Voluntary Program and organizations can interact through the following engagement channels:

- Regionally located DHS personnel from the Cyber Security Adviser (CSA) and Protective Security Adviser (PSA) programs. These personnel interact directly with organizations in their regions about cybersecurity and critical infrastructure protection.
- The Critical Infrastructure Partnership Advisory Council (CIPAC) Framework, a partnership between government and critical infrastructure sector owners and operators that enables a broad spectrum of activities to support and coordinate on critical infrastructure protection.
- Direct engagement between the C³ Voluntary Program and interested organizations. Organizations may access the C³ Voluntary Program website or contact the C³ Voluntary Program at cubedvp@hq.dhs.gov.
- Requests for Information (RFI), which create opportunities for the general public to provide input on cybersecurity solutions and policies.

Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing
Memorandum of February 15, 2015—Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems
By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.

Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this order is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.

Such information sharing must be conducted in a manner that protects the privacy and civil liberties of individuals, that preserves business confidentiality, that safeguards the information being shared, and that protects the ability of the Government to detect, investigate, prevent, and respond to cyber threats to the public health and safety, national security, and economic security of the United States.

This order builds upon the foundation established by Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), and Presidential Policy Directive–21 (PPD–21) of February 12, 2013 (Critical Infrastructure Security and Resilience).

Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive–1 (PPD–1) of February 13, 2009 (Organization of the National Security Council System), or any successor.

Sec. 2. Information Sharing and Analysis Organizations. [a] The Secretary of Homeland Security (Secretary) shall strongly encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs).

(b) ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities. ISAO membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities.

(c) The National Cybersecurity and Communications Integration Center (NCCIC), established under section 226(b) of the Homeland Security Act of 2002 (the “Act”), shall engage in continuous, collaborative, and inclusive coordination with ISAOs on the sharing of information related to cybersecurity risks and incidents, addressing such risks and incidents, and strengthening information security systems consistent with sections 212 and 226 of the Act.

(d) In promoting the formation of ISAOs, the Secretary shall consult with other Federal entities responsible for conducting cybersecurity activities,
including Sector-Specific Agencies, independent regulatory agencies at their
discretion, and national security and law enforcement agencies.

Sec. 3. ISAO Standards Organization. (a) The Secretary, in consultation
with other Federal entities responsible for conducting cybersecurity and
related activities, shall, through an open and competitive process, enter
into an agreement with a nongovernmental organization to serve as the
ISAO Standards Organization (SO), which shall identify a common set of
voluntary standards or guidelines for the creation and functioning of ISAOs
under this order. The standards shall further the goal of creating robust
information sharing related to cybersecurity risks and incidents with ISAOs
and among ISAOs to create deeper and broader networks of information
sharing nationally, and to foster the development and adoption of automated
mechanisms for the sharing of information. The standards will address the
baseline capabilities that ISAOs under this order should possess and be
able to demonstrate. These standards shall address, but not be limited to,
contractual agreements, business processes, operating procedures, technical
means, and privacy protections, such as minimization, for ISAO operation
and ISAO member participation.

(b) To be selected, the SO must demonstrate the ability to engage and
work across the broad community of organizations engaged in sharing
information related to cybersecurity risks and incidents, including ISAOs, and
associations and private companies engaged in information sharing in support
of their customers.

(c) The agreement referenced in section 3(a) shall require that the SO
gen in an open public review and comment process for the development of
the standards referenced above, soliciting the viewpoints of existing enti-
ties engaged in sharing information related to cybersecurity risks and inci-
dents, owners and operators of critical infrastructure, relevant agencies, and
other public and private sector stakeholders.

(d) The Secretary shall support the development of these standards and,
in carrying out the requirements set forth in this section, shall consult
with the Office of Management and Budget, the National Institute of Stan-
dards and Technology in the Department of Commerce, Department of Justice,
the Information Security Oversight Office in the National Archives and
Records Administration, the Office of the Director of National Intelligence,
Sector-Specific Agencies, and other interested Federal entities. All standards
shall be consistent with voluntary international standards when such inter-
national standards will advance the objectives of this order, and shall meet
the requirements of the National Technology Transfer and Advancement
Act of 1995 (Public Law 104–113), and OMB Circular A-119, as revised.

Sec. 4. Critical Infrastructure Protection Program. (a) Pursuant to sections
213 and 214(h) of the Critical Infrastructure Information Act of 2002, I
hereby designate the NCCIC as a critical infrastructure protection program
and delegate to it authority to enter into voluntary agreements with ISAOs
in order to promote critical infrastructure security with respect to cybersecu-

(b) Other Federal entities responsible for conducting cybersecurity and
related activities to address threats to the public health and safety, national
security, and economic security, consistent with the objectives of this order,
may participate in activities under these agreements.

(c) The Secretary will determine the eligibility of ISAOs and their members
for any necessary facility or personnel security clearances associated with
voluntary agreements in accordance with Executive Order 13549 of August
18, 2010 (Classified National Security Information Programs for State, Local,
Tribal, and Private Sector Entities), and Executive Order 12829 of January
6, 1993 (National Industrial Security Program), as amended, including as
amended by this order.

Sec. 5. Privacy and Civil Liberties Protections. (a) Agencies shall coordinate
their activities under this order with their senior agency officials for privacy
and civil liberties and ensure that appropriate protections for privacy and
civil liberties are incorporated into such activities. Such protections shall be based upon the Fair Information Practice Principles and other privacy and civil liberties policies, principles, and frameworks as they apply to each agency’s activities.

(b) Senior privacy and civil liberties officials for agencies engaged in activities under this order shall conduct assessments of their agency’s activities and provide those assessments to the Department of Homeland Security (DHS) Chief Privacy Officer and the DHS Office for Civil Rights and Civil Liberties for consideration and inclusion in the Privacy and Civil Liberties Assessment report required under Executive Order 13636.

Sec. 6. National Industrial Security Program. Executive Order 12829, as amended, is hereby further amended as follows:

(a) the second paragraph is amended by inserting “the Intelligence Reform and Terrorism Prevention Act of 2004,” after “the National Security Act of 1947, as amended,”;

(b) Sec. 101(b) is amended to read as follows: “The National Industrial Security Program shall provide for the protection of information classified pursuant to Executive Order 13526 of December 29, 2009, or any predecessor or successor order, and the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.).”;

(c) Sec. 102(b) is amended by replacing the first paragraph with: “In consultation with the National Security Advisor, the Director of the Information Security Oversight Office, in accordance with Executive Order 13526 of December 29, 2009, shall be responsible for implementing and monitoring the National Industrial Security Program and shall:”;

(d) Sec. 102(c) is amended to read as follows: “Nothing in this order shall be construed to supersede the authority of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.), or the authority of the Director of National Intelligence (or any Intelligence Community element) under the Intelligence Reform and Terrorism Prevention Act of 2004, the National Security Act of 1947, as amended, or Executive Order 12333 of December 8, 1981, as amended, or the authority of the Secretary of Homeland Security, as the Executive Agent for the Classified National Security Information Program established under Executive Order 13549 of August 18, 2010 [Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities].”;

(e) Sec. 201(a) is amended to read as follows: “The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Nuclear Regulatory Commission, the Director of National Intelligence, and the Secretary of Homeland Security, shall issue and maintain a National Industrial Security Program Operating Manual (Manual). The Secretary of Energy and the Nuclear Regulatory Commission shall prescribe and issue that portion of the Manual that pertains to information classified under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.). The Director of National Intelligence shall prescribe and issue that portion of the Manual that pertains to intelligence sources and methods, including Sensitive Compartmented Information. The Secretary of Homeland Security shall prescribe and issue that portion of the Manual that pertains to classified information shared under a designated critical infrastructure protection program.”;

(f) Sec. 201(f) is deleted in its entirety;

(g) Sec. 201(e) is redesignated Sec. 201(f) and revised by substituting “Executive Order 13526 of December 29, 2009, or any successor order,” for “Executive Order No. 12356 of April 2, 1982.”;

(h) Sec. 201(d) is redesignated Sec. 201(e) and revised by substituting “the Director of National Intelligence, and the Secretary of Homeland Security” for “and the Director of Central Intelligence.”;
(i) a new Sec. 201(d) is inserted after Sec. 201(c) to read as follows:

"The Manual shall also prescribe arrangements necessary to permit and enable secure sharing of classified information under a designated critical infrastructure protection program to such authorized individuals and organizations as determined by the Secretary of Homeland Security."

(j) Sec. 202(b) is amended to read as follows: "The Director of National Intelligence retains authority over access to intelligence sources and methods, including Sensitive Compartmented Information. The Director of National Intelligence may inspect and monitor contractor, licensee, and grantee programs and facilities that involve access to such information or may enter into written agreements with the Secretary of Defense, as Executive Agent, or with the Director of the Central Intelligence Agency to inspect and monitor these programs or facilities, in whole or in part, on the Director's behalf."

(k) Sec. 202(d) is redesignated as Sec. 202(o); and

(l) in Sec. 202 a new subsection (d) is inserted after subsection (c) to read as follows: "The Secretary of Homeland Security may determine the eligibility for access to Classified National Security Information of contractors, licensees, and grantees and their respective employees under a designated critical infrastructure protection program, including parties to agreements with such program; the Secretary of Homeland Security may inspect and monitor contractor, licensee, and grantee programs and facilities or may enter into written agreements with the Secretary of Defense, as Executive Agent, or with the Director of the Central Intelligence Agency, to inspect and monitor these programs or facilities in whole or in part, on behalf of the Secretary of Homeland Security."

Sec. 7. Definitions. (a) "Critical infrastructure information" has the meaning given in section 212(3) of the Critical Infrastructure Information Act of 2002.

(b) "Critical infrastructure protection program" has the meaning given the term in section 212(4) of the Critical Infrastructure Information Act of 2002.

(c) "Cybersecurity risk" has the meaning given the term in section 226(a)(1) of the Homeland Security Act of 2002 (as amended by the National Cybersecurity Protection Act of 2014).

(d) "Fair Information Practice Principles" means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(e) "Incident" has the meaning given the term in section 226(a)(2) of the Homeland Security Act of 2002 (as amended by the National Cybersecurity Protection Act of 2014).

(f) "Information Sharing and Analysis Organization" has the meaning given the term in section 212(5) of the Critical Infrastructure Information Act of 2002.

(g) "Sector-Specific Agency" has the meaning given the term in PPD-21, or any successor.

Sec. 8. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law or Executive Order to an agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law including those activities conducted with the private sector relating to criminal and national security threats. Nothing in this order shall be construed to provide an agency with authority for regulating
the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

THE WHITE HOUSE,
February 13, 2015.
<table>
<thead>
<tr>
<th>COMPONENT/SECTOR</th>
<th>AVIATION</th>
<th>MARITIME</th>
<th>FINANCIAL SERVICES</th>
<th>COMMUNICATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCATION OF INCORPORATION</td>
<td>Montreal, Canada</td>
<td>NC</td>
<td>Reston, VA</td>
<td>No physical location, but operated out of DHS Washington, DC offices</td>
</tr>
<tr>
<td>LEGAL STRUCTURE</td>
<td>Provided for in Eos 13691 and 13636 plus PPD-21</td>
<td>501c3 nonprofit organization</td>
<td>501c6 nonprofit organization</td>
<td>Government agency (a part of DHS)</td>
</tr>
<tr>
<td>PRIVATE SECTOR LEAD</td>
<td>Airports Council International</td>
<td>Maritime Security Council</td>
<td>American Bankers Association, Securities Industry Association</td>
<td>National Coordinating Center for Communications (NCC)</td>
</tr>
<tr>
<td>PRIVATE SECTOR PARTICIPANT</td>
<td>Aviation companies, manufacturers, and vendors</td>
<td>Ports, carriers, cruise lines, technology firms, government agencies, solution providers, importers/exporters</td>
<td>Banking firms and credit unions, securities firms, insurance companies, credit card companies, mortgage banking companies, financial services sector utilities and bureaus, appropriate industry associations, hedge fund IT, security service providers</td>
<td>30 individual telecomm companies providing telecomm or network services, equipment or software, and 3 associations</td>
</tr>
<tr>
<td>REPRESENTATIONAL COVERAGE</td>
<td>Five world regions: Africa, Europe, Latin America/Caribbean, Asia-Pacific, North America</td>
<td>Ocean carriers, cruise lines, port facilities and terminals, logistics providers, importers, exporters and related maritime industries throughout the world</td>
<td>Over 5,000 direct members and 30 member associations with the ability to reach 99% of the banks and credit unions and 85% of the securities industry, and nearly 50% of the insurance industry</td>
<td>24 Federal Government agencies and over 50 private sector communications and information technology companies</td>
</tr>
<tr>
<td>U.S.G. PARTNER</td>
<td>Department of Homeland Security (DHS)-Transportation Security Administration</td>
<td>DHS, Department of State, Coast Guard</td>
<td>Department of Treasury</td>
<td>DHS</td>
</tr>
<tr>
<td>ISAC OPERATOR</td>
<td>Air Domain Intelligence Integration Center</td>
<td>Maritime Security Council</td>
<td>Science Applications International Corporation (SAIC)</td>
<td>National Coordinating Center for Communications (NCC)</td>
</tr>
<tr>
<td>FUNDING</td>
<td>Sponsorship and membership fees</td>
<td>Membership fees</td>
<td>Entirely funded by the private sector</td>
<td>DHS</td>
</tr>
</tbody>
</table>


Chart 1
<table>
<thead>
<tr>
<th>COMPONENT/SECTOR</th>
<th>ELECTRICITY</th>
<th>EMERGENCY MANAGEMENT AND RESPONSE</th>
<th>INFORMATION TECHNOLOGY</th>
<th>CHEMICAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCATION OF INCORPORATION</td>
<td>GA</td>
<td>Emmitsburg, MD</td>
<td>VA</td>
<td>Washington, DC</td>
</tr>
<tr>
<td>LEGAL STRUCTURE</td>
<td>Nonprofit corporation</td>
<td>Government agency (US Fire Administration (USFA))</td>
<td>Nonprofit limited liability corporation (LLC)</td>
<td>American Chemical Council (ACC) members and individual subscribers</td>
</tr>
<tr>
<td>PRIVATE SECTOR LEAD</td>
<td>North American Electric Reliability Corporation (NERC)-Electricity Sub-Sector Coordinating Council</td>
<td>Fire Adapted Communities</td>
<td>Community Emergency Response Teams (CERTs)</td>
<td>ACC</td>
</tr>
<tr>
<td>PRIVATE SECTOR PARTICIPANT</td>
<td>Entities in the electricity sector, including the American Public Power Association and Canadian Electricity Association</td>
<td>All private fire safety supporting organizations as well as any group affiliated with the Voluntary Private Sector Preparedness Program</td>
<td>Vendor, manufacturer, or provider of IT (including Internet and e-commerce), products (hardware and software) solutions or services</td>
<td>The member companies of the 22 state chemical industry councils</td>
</tr>
<tr>
<td>REPRESENTATIONAL COVERAGE</td>
<td>90% of NERC members</td>
<td>Over 40,000 Emergency Services Sector (ESS) departments and agencies</td>
<td>70% IT globally, 85% cross-sector</td>
<td>All national critical infrastructure</td>
</tr>
<tr>
<td>U.S.G. PARTNER</td>
<td>Department of Energy, US Nuclear Regulatory Commission</td>
<td>USFA, FEMA, DHS</td>
<td>DHS</td>
<td>DHS</td>
</tr>
<tr>
<td>ISAC OPERATOR</td>
<td>NERC</td>
<td>ESS</td>
<td>Internet Security Systems</td>
<td>CHEMTREC</td>
</tr>
<tr>
<td>FUNDING</td>
<td>Federal funding</td>
<td>Tiered membership fees based on the level of service up to $40,000</td>
<td>Sponsorship from non-member organizations plus membership fees</td>
<td></td>
</tr>
<tr>
<td>COMPONENT/SECTOR</td>
<td>TRANSPORTATION (SURFACE)</td>
<td>WATER</td>
<td>TRANSPORTATION (PUBLIC)</td>
<td>REAL ESTATE</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------</td>
<td>-------</td>
<td>-------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>LOCATION OF INCORPORATION</td>
<td>Washington, DC</td>
<td>Washington, DC</td>
<td>Washington, DC</td>
<td>VA</td>
</tr>
<tr>
<td>LEGAL STRUCTURE</td>
<td>American Public Transportation Association (APTA) and Association of American Railroads (AAR) nonprofit organization</td>
<td>Nonprofit corporation</td>
<td>APTA nonprofit organization</td>
<td>Nonprofit corporation</td>
</tr>
<tr>
<td>PRIVATE SECTOR LEAD</td>
<td>APTA, AAR, Public Transit Sector Coordinator, Surface Transportation Sector Coordinator</td>
<td>Association of Metropolitan Water Agencies</td>
<td>APTA, AAR, Public Transit Sector Coordinator, Surface Transportation Sector Coordinator</td>
<td>The Real Estate Roundtable</td>
</tr>
<tr>
<td>PRIVATE SECTOR PARTICIPANT</td>
<td>Major North American freight railroads and AMTRAK, including the major Canadian and Mexican railroads and 480 short line railroads through the American Shortlines &amp; Regional Railroad Association (ASLRRRA)</td>
<td>Drinking water and wastewater utility managers</td>
<td>All American public transit programs</td>
<td>The Real Estate Roundtable, American Hotel &amp; Lodging Association, American Resort Development Association, Building Owners and Managers Association, International Council of Shopping Centers, National Apartment Association, National Association of Real Estate Investment Trusts, Real Estate Board of New York</td>
</tr>
<tr>
<td>REPRESENTATION AL COVERAGE</td>
<td>95% of North American freight railroad infrastructure</td>
<td>More than 40% of the nation's population</td>
<td>90% of persons using public transportation in the US</td>
<td>All 50 states and US territories</td>
</tr>
<tr>
<td>U.S.G. PARTNER</td>
<td>DHS, Department of Transportation (DOT)</td>
<td>DHS, EPA</td>
<td>DHS, DOT</td>
<td>DHS</td>
</tr>
<tr>
<td>ISAC OPERATOR</td>
<td>EWA Information and Infrastructure Technologies, Inc.</td>
<td>Self-operated</td>
<td>EWA Information and Infrastructure Technologies, Inc.</td>
<td>E-ISAC Traffic Light Protocol</td>
</tr>
<tr>
<td>FUNDING</td>
<td>Some federal funding</td>
<td>Membership fees up to $6,999 and matching contributions</td>
<td>Membership fees up to $6,999 and matching contributions</td>
<td>Membership fees</td>
</tr>
</tbody>
</table>

Chart 3
### INFORMATION SHARING ANALYSIS CENTERS (ISACS)

Susan Ginsburg (c) American Bar Association, Standing Committee on Law and National Security

Revised and adapted from a chart by Susan Eckert (2005)

<table>
<thead>
<tr>
<th>COMPONENT/SECTOR</th>
<th>RESEARCH AND EDUCATION</th>
<th>MULTI-STATE</th>
<th>SUPPLY CHAIN</th>
<th>HEALTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>FORMATION DATE</td>
<td>2003</td>
<td>2003</td>
<td>2006</td>
<td>2010</td>
</tr>
<tr>
<td>LOCATION OF INCORPORATION</td>
<td>N/A</td>
<td>NY</td>
<td>MA</td>
<td>FL</td>
</tr>
<tr>
<td>LEGAL STRUCTURE</td>
<td>Indiana University serves as its fiscal and administrative host organization</td>
<td>501c3 nonprofit organization</td>
<td>Corporation (segment of LO-JACK Corporation)</td>
<td>501c3 nonprofit organization</td>
</tr>
<tr>
<td>PRIVATE SECTOR LEAD</td>
<td>Global Research Network Operations Center (GR-NOC) at Indiana University</td>
<td>N/A</td>
<td>LO-JACK</td>
<td>SANS Institute</td>
</tr>
<tr>
<td>PRIVATE SECTOR PARTICIPANT</td>
<td>Colleges and universities, teaching hospitals, research and education network providers, and government-funded research organizations</td>
<td>State government, local government, territories, tribes</td>
<td>Supply chain companies, including manufacturers and shippers, cargo carriers (air, rail, highway and maritime), consignees, supply chain service suppliers, law enforcement and federal government agencies</td>
<td>Healthcare providers (hospitals, clinics, pharmaceutical organizations, BioTech companies, public health departments, labs and blood banks, health insurers, medical device manufacturers, health sector tech and security companies, home health care agencies, ambulatory facilities, federal homes, long term care facilities)</td>
</tr>
<tr>
<td>REPRESENTATIONAL COVERAGE</td>
<td>400+ educational institutions</td>
<td>39,000 municipalities and fusion centers over all 50 states, DC, and the five territories</td>
<td>See above</td>
<td>Entire US healthcare sector, especially wrt cybersecurity</td>
</tr>
<tr>
<td>U.S.G. PARTNER</td>
<td>DHS</td>
<td>DHS</td>
<td>DHS</td>
<td>Department of Health and Health Services</td>
</tr>
<tr>
<td>ISAC OPERATOR</td>
<td>Center for Internet Security (CIS) Security Operations Center</td>
<td>Supply Chain Integrity, Inc.</td>
<td>Global Situational Awareness Center</td>
<td></td>
</tr>
<tr>
<td>FUNDING</td>
<td>Membership fees and contribution form</td>
<td>Federal funding and membership fees</td>
<td>Annual member subscription dues</td>
<td>Membership fees up to $25,000</td>
</tr>
</tbody>
</table>

Chart 4
<table>
<thead>
<tr>
<th>COMPONENT/SECTOR</th>
<th>OIL AND GAS</th>
<th>OVER THE ROAD AND BUS</th>
<th>DEFENSE INDUSTRIAL BASE (DIB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FORMATION DATE</td>
<td>Jun. 2014</td>
<td>2014</td>
<td>N/A</td>
</tr>
<tr>
<td>LOCATION OF INCORPORATION</td>
<td>DE</td>
<td>Herndon, VA</td>
<td>Huntsville, AL</td>
</tr>
<tr>
<td>LEGAL STRUCTURE</td>
<td>501c3 nonprofit organization</td>
<td>Government agency given grant money by DHS, works in conjunction with the surface and public transportation ISACs</td>
<td>N/A</td>
</tr>
<tr>
<td>PRIVATE SECTOR LEAD</td>
<td>Retail Industry Leaders Association and National Retail Federation</td>
<td>APTA, AAR, Public Transit Sector Coordinator, Surface Transportation Sector Coordinator</td>
<td>DIB Sector Coordinating Council (SCC)</td>
</tr>
<tr>
<td>PRIVATE SECTOR PARTICIPANT</td>
<td>Integrated oil companies, natural gas companies, upstream companies, mid-stream companies, downstream companies, appropriate industry associations, energy service and supply companies, supporting ONG industry segments</td>
<td>See above</td>
<td>Aerospace Industries Association, American Society for Industrial Security, Industrial Security Working Group, National Classification Management Society, National Defense Industrial Association</td>
</tr>
<tr>
<td>REPRESENTATIONAL COVERAGE</td>
<td>All oil and natural gas industry companies (public and private) and recognized trade associations that have a proven, active presence in North America</td>
<td>Government and other critical infrastructure ISACs in the United States dealing with the &quot;technical sector&quot;</td>
<td>100,000 US companies and subcontractors</td>
</tr>
<tr>
<td>U.S.G. PARTNER</td>
<td>ICS-CERT</td>
<td>DHS, DOT</td>
<td>DHS, Department of Defense</td>
</tr>
<tr>
<td>ISAC OPERATOR</td>
<td>Self-operated</td>
<td>EWA Information and Infrastructure Technologies, Inc.</td>
<td>Defense Security Information Exchange</td>
</tr>
<tr>
<td>FUNDING</td>
<td>Membership fees based on organization's annual revenue</td>
<td>Some federal funding</td>
<td>Membership fees ($2,000 annually)</td>
</tr>
</tbody>
</table>
The Electric Industry Gets Serious About Cybersecurity

Fun with the EO, PD, DHS, NIST, NERC, ESCC, ES-ISAC, DOE, and FERC

Jonathan Schneider
Stinson Leonard Street
Jschneider@stinson.com

Homeland Security Law Institute
August 28, 2015
Background

- Evidence of the nation’s cyber vulnerability has increased geometrically over the past five years.

- 2013 Mandiant report of the concerted effort apparently mounted by China’s military was eye-opening.

- Recent CrowdStrike report details Chinese military strikes at government, military contractor, and research facilities in satellite and space industries.

- High profile incidents pointing to potential destructive potential include:
  - Shamoon attack on Saudi Aramco disabled 30,000 computers
  - 23 attacks on US Pipeline systems in 2012
  - Dozens of attacks on financial institutions in 2012 (DHS report)
  - Major Denial of Service attack successfully brought down internet service to Jacksonville Electric Authority in late-2013
  - May, 2014 – ICS-CERT reported successful intrusion into internet-facing utility control system through password compromised by brute-force attack.
  - North Korean hackers attack Sony Pictures (November 2014)
  - Cyber attacks infiltrate United Airlines; U.S. health insurer Anthem (2015)
  - Hackers believed to be associated with Chinese government infiltrate U.S. Office of Personnel Management – potentially affecting up to 18 million federal workers (June 2015)
  - Russian cyber attack targets Pentagon/DOD e-mail systems (July 2015)

- Idaho Labs Aurora Test shows you can blow up a power plant remotely.

- Soviet Invasion of Georgia - Potential for full-out cyber warfare demonstrated

- Former Secretary of Defense Leon Panetta warned of potential for a “Cyber Pearl Harbor.”

- President Obama has declared cyber threats to be among the most serious economic and national security challenges the nation faces.
10/2012 Report – Energy sector has been a focal point
- 40% of all cyber attacks in 2012
- 59% in 2013
Department of Homeland Security - Industrial Control Systems
Cyber Emergency Response Team (ICS-CERT)

Energy Sector continue to be a focal point for attacks

FY 2014 Incidents Reported by Sector (245 total):

- Critical Manufacturing: 65, 27%
- Energy: 79, 32%
- Communications: 14, 6%
- Commercial Facilities: 7, 3%
- Chemical: 4, 2%
- Unknown: 6, 2%
- Water: 14, 6%
- Transportation: 12, 5%
- Nuclear: 6, 2%
- Information Technology: 5, 2%
- Healthcare: 15, 6%
- Government Facilities: 13, 5%
- Finance: 3, 1%
- Food and Ag: 2, 1%

Source: ICS-CERT Year in Review – 2014, pg. 6
Understanding Cyber Vulnerabilities

- **Attack Vectors**
  - Internet access (hacking)
  - Phishing (email)
  - Watering Hole Attacks (logging on to mined websites)
  - Inserted malware (Stuxnet and reversed engineered versions)
  - Mobile device attacks
  - Internal exposure

- **Electric Sector Vulnerabilities**
  - **Operations/Control Systems**
    - Idaho Labs Aurora Test – Industry wake-up call
    - Televant (project files for OASyS SCADA system stolen)
  - **Communications and Information Systems**
    - Communications: JEA Denial of Internet Service
    - Theft (proprietary data – Nortel, banking)
FY 2014 Incidents Reported by Access Vector (245 total)

- Miscellaneous: 21, 9%
- Weak Authentication: 13, 5%
- Network Scanning/Probing: 53, 22%
- Removable Media: 5, 2%
- Brute Force Intrusion: 3, 1%
- Abuse of Access Authority: 9, 4%
- Spear Phishing: 42, 17%
- SQL Injection: 5, 2%
- Unknown: 94, 38%

Source: ICS-CERT Year in Review – 2014, pg. 7
Legislative Gridlock

- Numerous bills introduced in Congress over the past six years, and dozens of amendments

- Most legislative activity targeted energy industry
  - Ironically, energy industry may be better protected through NERC standards than any other sector

- Legislative focus now encompasses other major economic, physical infrastructure and manufacturing sectors – to stop threats to national security, and theft of trade secrets

  - **Cybersecurity Information Sharing Act of 2015 (CISA):**
    - Aims to offer legal protections to companies that would encourage sharing of information on networks & cyber threat vulnerabilities with government
    - Passed House in April, 2015; Withdrawn from consideration by Senate until September 2015

- Electric Industry Supports:
  - Information Sharing – Govt. to Industry
  - Emergency Directives
  - Liability Protection

- Electric Industry Opposes:
  - Redundant mandatory standards
  - Disruption of Industry-based (NERC) Standards Development Process
White House Response to Legislative Gridlock

- White House stepped into the legislative void on February 12, 2013 with its Executive Order (“Improving Critical Infrastructure Cybersecurity”)

- Executive Order sets up a broad program:
  - Provides for information sharing by federal agencies w/owners of critical assets
  - Cybersecurity Framework to be promulgated by the National Institute of Standards and Technology (NIST)
    - A “voluntary framework” for managing cyber vulnerabilities
    - Preliminary draft was due 10/10/13
Who’s in the Mix?

• Federal Energy Regulatory Commission (FERC)
  • North American Electric Reliability Corporation (NERC)
• Department of Homeland Security (DHS)
• Department of Energy (DOE)
• White House
  • Presidential Orders and Directives addressed to Dep’t of Commerce (acting through the National Institute of Standards and Technology, NIST)
Electric Sub-Sector Coordinating Council


- Broad Aim: High level industry interface with top levels of government.

- Charter lists responsibilities including:
  - Coordination of policy development with other sectors;
  - Representation of electric sector to Homeland Security, Critical Infrastructure Partnership Advisory Council and Working Groups;
  - Improvement in timely and actionable information sharing within industry and between industry and government.
  - Review of CIP related plans and policies;
  - Coordination between government and industry on preparedness, incident response, recovery, lessons learned, best practices.

- Composition of ESCC: (1) Industry Execs; (2) NERC CEO

- Support provided by NERC
Electricity Sector Information Sharing and Analysis Center (ES-ISAC)


- **Mission:** establishes situational awareness, incident management, coordination and communication capabilities within the electricity sector through timely, reliable and secure information exchange. In collaboration with the DOE and ESCC, serves as the primary security communications channel facilitating response to cyber and physical threats, vulnerabilities and incidents.

- **Activities**
  - Facilitates information sharing re: physical and cyber threats, vulnerabilities, protective practices;
  - Rapid response through contact and coordination
  - Receives incident data from private and public sources
  - Shares threat alerts, warning, advisories, notices
  - Coordination with other ISACs
  - Awareness of private-government Infrastructure interdependencies.
  - Outreach-education to electric sector

- **Logistical support:** NERC
NERC’s Story: The Tale Of Two Blackouts

November 9, 1965          August 14, 2003
FPA Section 215 - Statutory Basics
A Few Observations

- Congress enacted mandatory reliability regime with full industry support - Energy Policy Act of 2005

- Congress rejected FERC-centric regime in favor of an ERO (designated by FERC) required to consider industry stakeholder input in:
  - Choosing board of trustees
  - Populating committees
  - Promulgating Reliability Standards (including cybersecurity)

- Relationship with Industry is complicated: The ERO must be independent of industry, but it depends on industry for the content of the standards.

- Relationship with FERC is complicated:
  - NERC is overseen by FERC – which approves standards and can reverse enforcement actions.
  - NERC occupies the same space as FERC, which:
    - is also authorized to direct NERC to develop specific standards; and
    - may undertake its own enforcement actions.

(a)(4): The term “reliable operation” means operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.

(b) Jurisdiction and applicability (1) The Commission [FERC] shall have jurisdiction, within the United States, over the ERO [Electric Reliability Organization] certified by the Commission under subsection (c) of this section, any regional entities, and all users, owners and operators of the bulk-power system, including but not limited to the entities described in section 201(f) for purposes of approving reliability standards established under this section and enforcing compliance with this section. All users, owners and operators of the bulk-power system shall comply with reliability standards that take effect under this section.
Federal Power Act Section 215, Statutory Basics – FERC Oversight

- FERC Oversight of ERO:
  - Approves Standards under statutory standards
  - Considers appeals of enforcement actions
- FERC orders subject to appeal under Federal Power Act
NERC Compliance & Enforcement Organization

- FERC
- NERC
  - Regional Oversight-Compliance
  - Compliance Analysis & Certification
  - Compliance Enforcement

8 Regional Entities
Critical Infrastructure Protection ("CIP") Under NERC Standards

- CIP-002-5 – BES Cyber System Categorization - identification and risk-based ranking of 'BES Cyber Systems' (NOTE: V.5 not effective until 4/16)

- Definitions:
  
  - BES ‘Cyber System’ defined as ‘one or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks.’
  
  - ‘Cyber Assets’ – Programmable electronic devices, including hardware, software and data
  
  - ‘BES Cyber Assets’ - are those that ‘if rendered unavailable, degraded or misused would, within 15 minutes of required operation....adversely impact one or more facilities....which if ...unavailable, would affect the reliable operation of the Bulk Electric System.’ [subject to one year study]

- Impact Ranking of Cyber Systems - High, Medium and Low
V. 5: Categorizes ALL BES Cyber Systems (Impact Rating Criteria):

- High Impact: BES Systems located at Large Control Centers (Reliability Coordinators; BAs with generation aggregating to 3000 MW); specified Transmission and Generation

- Medium Impact: Generation and Transmission + smaller control centers
  - Generation aggregated to 1500 MW or higher
  - Transmission at 500 kV or higher or between 200 and 499, where it aggregates at a weighted average value of 3000.

- Low Impact: All other BES Cyber Systems

NOTE: FERC directed NERC to: (1) develop objective criteria for evaluating protection systems for low impact assets; and (2) require entities to identify assets

NOTE: Applicability to limited Distribution Facilities: Underfrequency Load shedding or Undervoltage Load shedding; Special Protection Systems
Existing Protection:
Critical Infrastructure Protection under North American Electric Reliability Corporation (NERC) Standards

- **CIP-003-5 – Security Management Controls**
  - Utilities must maintain/implement/document cybersecurity policies addressing requirements of CIP 4 – 11.
  - More prescriptive and routinized than V. 3

- **CIP-004-5 – Personnel & Training – training, awareness and personnel risk assessment**

- **CIP-005-5 – Electronic Security Perimeters**
  - High and medium impact Cyber Systems connected to network via routable protocol (network address allowing inter-network communication) must reside behind an “electronic security perimeter” (secure access)
  - External routable connectivity must be via protected Electronic Access Point accompanied by method for detecting malicious communication.
Existing Protection:
Critical Infrastructure Protection under North American Electric Reliability Corporation (NERC) Standards

- **CIP-006-5** – Physical Security of Cyber System Assets
  - Secure physical access to high and medium impact Cyber System Assets

- **CIP-007-5** – Systems Security Management
  - Port management
  - Security Patch Management
  - Malicious Software Prevention
  - Authenticate users (authorized access)
  - Security status monitoring

- **CIP-008-5** – Incident Reporting and Response Planning
  - Process for identifying, reporting and responding to cyber incidents
  - ES-ISAC must be notified w/in one hour (change from V.3)

- **CIP-009-5** – Recovery Plans for Critical Cyber Assets
  - Responsible entities must devise, document, implement and test (full operational exercise) recovery plans.
Existing Protection:
Critical Infrastructure Protection under North American Electric Reliability Corporation (NERC) Standards

- **CIP-010-5 (New) – Configuration Change Management and Vulnerability.**
  - **Purpose:** to detect and prevent unauthorized changes to BES Cyber systems by specifying configuration change management and vulnerability assessment.
  - Baseline configuration tracked; process for making changes documented and verified.
  - Active vulnerability assessment.

- **CIP-011-5 (New) – Information Protection**
  - **Purpose:** To prevent unauthorized access to BES Cyber system information by specifying information protection requirements.
Upcoming Changes to CIP V. 5

- Removal of “Identify, Assess, Correct” language
  - “Reliability Assurance Initiative” to Cover (June, 2014 filing)

- Low Impact Assets (June, 2014 filing)
  - NERC to administer objective criteria for evaluating protections
  - Registered Entities to develop ability to identify nature and location of assets for audit and compliance purposes

- Communications Networks – NERC to develop definition and propose standards (December, 2014)

- Transient Devices (thumb drives, etc.) - New or revised standards are directed to address vulnerabilities.
Physical Security

- **April 2013**: sniper attack at PG&E’s Metcalf transmission substation
  - Shooting for 19 minutes; “surgically” knocked out 17 transformers
  - CAISO was able to avoid any blackouts

- **2/5/14**: WSJ article provides a detailed account and quotes former FERC Chair:
  - Metcalf attack was "the most significant incident of domestic terrorism involving the grid that has ever occurred"

- Mounting Congressional pressure on FERC (and NERC)

- **3/7/14**: FERC Directive to NERC issued

- **5/23/14**: NERC filed proposed standard, following industry collaboration

- **7/17/14**: FERC issued NOPR proposing to approve standard, with modifications.
Physical Security

• The standard calls for entities registered with NERC as Transmission Owners or Operators to:

  1. Perform risk assessments identifying critical transmission stations, substations and associated primary control centers;

  2. Evaluate physical attack vulnerabilities of those facilities; and

  3. Develop and implement plans to protect against attacks.

• Risk assessments and security plans will be subject to third-party verification (by region, NERC, et al.)

• Initial assessment performed by entities operating at over 200 kV at a single station or substation, and where the station or substation is connected at voltages of 200 kV or higher, while meeting specified aggregated weighted values
DOE’s Cybersecurity Capability Maturity Model 1.1 (ES – C2M2) (Feb. 2014):

- Voluntary Framework – Result of Gov’t-Industry Collaboration
- Ten Core Domains (Competencies)
  1. Risk Management;
  2. Asset, Change, and Configuration Management;
  3. Identity and Access Management;
  4. Threat and Vulnerability Management;
  5. Situational Awareness;
  6. Information Sharing and Communications;
  7. Event and Incident Response, Continuity of Operations;
  8. Supply Chain and External Dependencies Management;
  9. Workforce Management; and
  10. Cybersecurity Program Management

- Maturity Levels (Process Oriented Approach, geared to each domain): (1) Initiation; (2) certain degree of performance including program documentation, stakeholder involvement, resource commitment and reliance on standards or guidelines; and (3) a fully managed program, reflecting evolving risks.
Headline News: Without legislation, the White House has directed the Secretary of Homeland Security, the Attorney General, DOD, and the NIST (National Institute of Standards and Technology) to implement a broad program ensuring:

- Information Sharing by Governmental Agencies with private sector regarding cyber threats
- The identification of Critical Infrastructure at risk
- The creation of a “voluntary” Critical Infrastructure Cybersecurity baseline program ("the Framework") by NIST -
Application to Industries and Responsible Sector-Specific Agencies

- Chemical: Department of Homeland Security
- Commercial Facilities: Department of Homeland Security
- Communications: Department of Homeland Security
- Critical Manufacturing: Department of Homeland Security
- Dams: Department of Homeland Security
- Defense Industrial Base: Department of Defense
- Emergency Services: Department of Homeland Security
- **Energy**: Department of Energy
- Financial Services: Department of the Treasury
- Food and Agriculture: U.S. Department of Agriculture and Department of Health and Human Services
- Government Facilities: Department of Homeland Security and General Services Administration
- Healthcare and Public Health: Department of Health and Human Services
- Information Technology: Department of Homeland Security
- Nuclear Reactors, Materials, and Waste: Department of Homeland Security
- Transportation Systems: Department of Homeland Security and Department of Transportation
- Water and Wastewater Systems: Environmental Protection Agency
What Is Critical Infrastructure?

- **Executive Order defined Critical Infrastructure to mean:** “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

- **Identification of assets deemed most critical:**
  - Within 150 days of the date of the Executive Order (mid-July, 2013), the Secretary shall use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

- Assets were tentatively identified through a “consultative process,” but final cut is a work in progress.
NIST Cybersecurity Baseline Program ("The Framework")

- **Goal of The Framework**: “To establish a common language to address and manage cybersecurity without added regulatory requirements.”

- **Components**:
  - **Framework Core** - Substantive activities and outcomes
  - **Framework Tiers** - Levels of cybersecurity risk management, rigor and sophistication
  - **Framework Profile** – Internal description of current and desired state of cybersecurity risk protection, reflecting risk tolerance, legal/regulatory requirements
Framework Core

<table>
<thead>
<tr>
<th>Functions</th>
<th>Categories</th>
<th>Subcategories</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROTECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DETECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RESPOND</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECOVER</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Framework Core

<table>
<thead>
<tr>
<th>Functions</th>
<th>Meaning</th>
<th>Categories</th>
<th>Subcategories (selected)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.</td>
<td>Asset Management</td>
<td>• Physical and systems inventory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Resource priority</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Intra-org responsibilities</td>
</tr>
<tr>
<td></td>
<td>Understanding the business context, the resources that support critical functions, and the related cybersecurity risks.</td>
<td>Business Environment</td>
<td>• Supply chain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Place in industry sector and critical infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Priorities</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Dependencies</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Resilience requirements</td>
</tr>
<tr>
<td></td>
<td>Enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business</td>
<td>Governance</td>
<td>• Information security policy, roles and responsibilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Legal and regulatory requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Governance and risk management</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>• Identify asset vulnerabilities</td>
<td>Risk Assessment</td>
<td>• Identify asset vulnerabilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Information sharing forums</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Risk and responses identified and prioritized</td>
</tr>
<tr>
<td>Risk Management</td>
<td>• Processes established, managed</td>
<td></td>
<td>• Processes established, managed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Organization risk tolerance assessed/expressed</td>
</tr>
</tbody>
</table>
## Framework Core

<table>
<thead>
<tr>
<th>Functions</th>
<th>Meaning</th>
<th>Categories</th>
<th>Subcategories (selected)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protect</strong></td>
<td>Develop and implement appropriate safeguards for delivery of services</td>
<td><strong>Access Control</strong></td>
<td>• Physical and electronic access controlled – on site and remote</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Awareness and Training</strong></td>
<td>• All users, including third parties and senior executives</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Data Security</strong></td>
<td>• Data at rest protected</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Data in transit protected</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Assets managed through removal, transfer, disposition</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Data leaks protected</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Integrity checking for software</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Information Protection</strong></td>
<td>• Baseline configuration maintained</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Processes and procedures</strong></td>
<td>• System development life cycle</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Configuration change control processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Backup information</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Physical protection</td>
</tr>
<tr>
<td><strong>Maintenance</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Protective Technology</strong></td>
<td></td>
<td></td>
<td>• Removable devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Communication and control networks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• System access limited</td>
</tr>
</tbody>
</table>
## Framework Core

<table>
<thead>
<tr>
<th>Functions</th>
<th>Meaning</th>
<th>Categories</th>
<th>Subcategories (selected)</th>
</tr>
</thead>
</table>
| Detect    | Develop and implement activities to timely identify the occurrence of cybersecurity events | Anomalies and Events | • Detected events analyzed  
• Impact of events determined  
• Incident alert threshold established |
|           |         | Continuous Security Monitoring | • Network monitored  
• Personnel Activity monitored  
• Physical plant monitored  
• Malicious code detected  
• Unauthorized mobile code detected  
• External service provider monitored  
• Monitoring for unauthorized personnel, connections, devices |
|           |         | Detection Processes | • Roles and responsibilities  
• Testing detection systems  
• Communication |
## Framework Core

<table>
<thead>
<tr>
<th>Functions</th>
<th>Meaning</th>
<th>Categories</th>
<th>Subcategories (selected)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Respond</strong></td>
<td>Develop and implement activities to take action in response to cybersecurity event</td>
<td><strong>Response Planning</strong></td>
<td>• Physical and electronic access controlled – on site and remote</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Communications</strong></td>
<td></td>
</tr>
</tbody>
</table>
|           |         | **Analysis** | • Notifications from Detection systems analyzed  
• Impact understood  
• Forensics undertaken |
|           |         | **Mitigation** | • Incidents contained and mitigated |
|           |         | **Improvements** | • Implement lessons learned |
### Framework Core

<table>
<thead>
<tr>
<th>Functions</th>
<th>Meaning</th>
<th>Categories</th>
<th>Subcategories (selected)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recover</td>
<td>Develop and implement appropriate activities to maintain plans or resilience and to restore capability and service.</td>
<td>Recovery planning</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Improvements</td>
<td></td>
</tr>
</tbody>
</table>
|           |         | Communications | • PR managed (!)  
• Reputation repair  
• Recovery activity communicated to internal stakeholders |
“Implementation Tiers”

- **Tier 1 – Partial**
  - **Risk Management Process** – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.
  - Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
  - **Integrated Risk Management Program** – There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established.

- **Tier 2 – Risk Informed**
  - **Risk Management Process** – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
  - **Integrated Risk Management Program** – There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis.
  - **External Participation** – The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.
Cyber Framework
“Implementation Tiers”

- **Tier 3 – Repeatable**
  - *Risk Management Process* – The organization’s risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
  
  - *Integrated Risk Management Program* – There is an organization-wide approach to managing cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.
  
  - *External Participation* – The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.

- **Tier 4 – Adaptive**
  - All of the above, plus:
  
  - Organization updates its practices based on lessons learned and predictive indicators. Continuous improvement and active adaptation to changing risks.
  
  - Organizational culture reflects risk management philosophy
  
  - Active information sharing
Organization “Profile” under the Framework

- The Profile is “the alignment of Functions, Categories and Subcategories with business requirements, risk tolerance and resources of the organization.”
- Creation of Profile follows from senior management direction re: priorities, resources and risk tolerance to business processes and operations. Feedback loop follows development of Profile at operating level.
- In so many words, the Profile is designed to describe where an organization is and where it wants to be.
Coordination of Framework Implementation
Implementing the Framework: Department of Energy

- DOE “Glossy” points to Framework/C2M2 Overlap
  - Framework Core compares with C2M2 “Domains”
  - Framework “Tiers” overlap C2M2 “Maturity levels”

- DOE at work on detailed implementation guidance
  - Recommends that C2M2 be used as a tool to implement the Framework
  - DOE will NOT map the Framework to CIP Standards
The Framework is Voluntary, but cannot reasonably be ignored

- The Framework is “Voluntary”

- It will inevitably be relevant for these purposes:
  - Liability in the event of harm – standard of care
  - Regulatory obligations and investigations
  - Insurance Markets
  - Financial Risk Disclosure
What Must Asset Owners Do and What Should They Do?

- Critical Infrastructure owners/operators must:
  - Comply with CIP Requirements
  - Determine whether to participate in the Framework
  - Weigh risks of non-participation
    - Potential liability in not meeting benchmark
    - Possible Disclosure Issue
  - Liability Implications are important – Standard of Care Established
    - Insurance Markets Likely to Be Affected
- Asset owners should consider application of CIP Standards and Framework to non-BES and non-Critical Assets
“You all know General Petersen from I.T.”
NATIONAL STRATEGY FOR GLOBAL SUPPLY CHAIN SECURITY

JANUARY 2012
The United States and nations around the world depend upon the efficient and secure transit of goods through the global supply chain system. In recent years, advances in communications technology, along with reductions in trade barriers and production costs, have opened new markets and created new jobs and opportunity for workers. The global supply chain system that supports this trade is essential to the United States’ economy and security and is a critical global asset.

We have seen that disruptions to supply chains caused by natural disasters – earthquakes, tsunamis, and volcanic eruptions – and from criminal and terrorist networks seeking to exploit the system or use it as a means of attack can adversely impact global economic growth and productivity. As a nation, we must address the challenges posed by these threats and strengthen our national and international policies accordingly.

Through the National Strategy for Global Supply Chain Security, we seek to strengthen global supply chains in order to protect the welfare and interests of the American people and secure our Nation’s economic prosperity. We reject the false choice between security and efficiency and firmly believe that we can promote economic growth while protecting our core values as a nation and as a people. Through this Strategy, we endorse a national approach and active collaboration with the international community. We will integrate and energize our efforts to enhance our ability to manage risk by building a layered defense, addressing threats early, and fostering a resilient system that can absorb and recover rapidly from unanticipated disruptions. By institutionalizing information-sharing arrangements, streamlining government processes, and synchronizing standards and procedures, we can realize new efficiencies while strengthening global supply chains.

The Federal Government cannot achieve this alone. Partnerships with state, local, and tribal governments, the private sector, and the international community are critical to realizing our shared goal of building a new framework to strengthen and protect this vital system.
# Table of Contents

- Executive Summary .................................................. 1
- Introduction ............................................................. 2
- Our Strategic Goals ..................................................... 2
- Our Strategic Approach ............................................... 3
- The Path Forward ....................................................... 5
- Conclusion .............................................................. 6
Executive Summary

International trade has been and continues to be a powerful engine of United States and global economic growth. In recent years, communications technology advances and trade barrier and production cost reductions have contributed to global capital market expansion and new economic opportunity. The global supply chain system that supports this trade is essential to the United States’ economy and is a critical global asset.

Through the National Strategy for Global Supply Chain Security (the Strategy), we articulate the United States Government’s policy to strengthen the global supply chain in order to protect the welfare and interests of the American people and secure our Nation’s economic prosperity. Our focus in this Strategy is the worldwide network of transportation, postal, and shipping pathways, assets, and infrastructures by which goods are moved from the point of manufacture until they reach an end consumer, as well as supporting communications infrastructure and systems. The Strategy includes two goals:

Goal 1: Promote the Efficient and Secure Movement of Goods – The first goal of the Strategy is to promote the timely, efficient flow of legitimate commerce while protecting and securing the supply chain from exploitation, and reducing its vulnerability to disruption. To achieve this goal we will enhance the integrity of goods as they move through the global supply chain. We will also understand and resolve threats early in the process, and strengthen the security of physical infrastructures, conveyances and information assets, while seeking to maximize trade through modernizing supply chain infrastructures and processes.

Goal 2: Foster a Resilient Supply Chain – The second goal of the Strategy is to foster a global supply chain system that is prepared for, and can withstand, evolving threats and hazards and can recover rapidly from disruptions. To achieve this we will prioritize efforts to mitigate systemic vulnerabilities and refine plans to reconstitute the flow of commerce after disruptions.

Our approach is informed by the following guiding principles:

- **Galvanize Action** – Integrate and spur efforts across the United States Government, as well as with state, local, tribal and territorial governments, the private sector and the international community.

- **Manage Supply Chain Risk** – Identify, assess, and prioritize efforts to manage risk by utilizing layered defenses, and adapting our security posture according to the changing security and operational environment.

In support of the Strategy, at the Federal level, we will update our threat and risk assessments; align programs and resources; and engage government, private sector, and international stakeholders. The purpose of this engagement is to seek specific recommendations to inform and guide our collaborative implementation of the Strategy.
Introduction

The global supply chain provides the food, medicine, energy, and products that support our way of life. Many different entities are responsible for or reliant upon the functioning of the global supply chain, including regulators, law enforcement, public-sector buyers, private-sector businesses, and other foreign and domestic partners. The global system relies upon an interconnected web of transportation infrastructure and pathways, information technology, and cyber and energy networks. While these interdependencies promote economic activity they also serve to propagate risk across a wide geographic area or industry that arises from a local or regional disruption.

The United States Government, in collaboration with state, local, tribal, international and private sector stakeholders, has undertaken a number of efforts to strengthen the global supply chain. These efforts include implementation of legislative requirements and a number of strategic efforts with a specific security focus. This Strategy incorporates and builds upon those prior efforts.

Our Strategic Goals

We seek to create and protect a global supply chain system that supports innovation and prosperity by securely and reliably moving goods within our domestic borders and around the world in a timely manner. We must both protect the current system's continuity, while simultaneously building for the future by implementing effective and cost-efficient measures that will strengthen the system and expedite the movement of lawful global commerce.

Goal 1: Promote the Secure and Efficient Movement of Goods

We all share a collective interest in promoting the timely, efficient flow of legitimate commerce while protecting and securing the supply chain from exploitation, and reducing its vulnerability to disruption. By linking security and efficiency under a single goal, the United States Government seeks to emphasize that security is an essential element of an efficient and functioning supply chain system.

To accomplish our goal, the United States Government will seek to:

- **Resolve threats early** to expedite the flow of legitimate commerce. By integrating security processes into supply chain operations, we can identify items of concern and seek to resolve them as early in the process as possible.

---

1. Supply chain-related legislation includes the Security and Accountability for Every Port (SAFE Port) Act, the Maritime Transportation Security Act, the Aviation and Transportation Security Act, the Implementing Recommendations of the 9/11 Commission Act, and others.
2. See, e.g., the National Strategy to Combat Transnational Organized Crime (July 2011), the National Strategy for Counterterrorism (June 2011), the updated Strategy for American Innovation (February 2011), the Global Nuclear Detection Architecture Strategic Plan (December 2010), the Joint Strategic Plan on Intellectual Property Enforcement (June 2010), the National Security Strategy (May 2010), the International Strategy for Cyberspace (May 2010), the Surface Transportation Security Priority Assessment (March 2010), the Quadrennial Homeland Security Review (February 2010), the Framework for Revitalizing American Manufacturing (December 2009), the National Strategy for Aviation Security (March 2007) and its supporting plans, the National Strategy for Pandemic Influenza (November 2005), the National Strategy for Maritime Security (September 2005) and its supporting plans, and the National Strategy to Combat Weapons of Mass Destruction (December 2002).
• **Improve verification and detection** capabilities to identify those goods that are not what they are represented to be, are contaminated, are not declared, or are prohibited; and to prevent cargo from being compromised or misdirected as it moves through the system.

• **Enhance security of infrastructure and conveyances** in order to protect the supply chain and critical nodes, through limiting access to cargo, infrastructure, conveyances, and information to those with legitimate and relevant roles and responsibilities.

• **Maximize the flow of legitimate trade** by modernizing supply chain infrastructure and processes to meet future market opportunities; developing new mechanisms to facilitate low risk cargo; simplifying our trade compliance processes; and refining incentives to encourage enhanced stakeholder collaboration.

**Goal 2: Foster a Resilient Supply Chain**

Integrated supply chains are fast and cost-efficient but also susceptible to shocks that can rapidly escalate from localized events into broader disruptions. We will seek to develop a global supply chain system that is prepared for and can withstand evolving threats and hazards and can recover rapidly from disruptions. Increased resilience and flexible, dynamic capabilities will improve the Nation’s ability to absorb shocks, save lives, and reduce the overall impact of a disruption.

To accomplish our goal, the United States Government will seek to:

• **Mitigate systemic vulnerability** to a supply chain disruption prior to a potential event by using risk management principles to identify and protect key assets, infrastructure, and support systems; and promoting the implementation of sustainable operational processes and appropriate redundancy for those assets.

• **Promote trade resumption policies and practices** that will provide for a coordinated restoration of the movement of goods following a potential disruption by developing and implementing national and global guidelines, standards, policies, and programs.

**Our Strategic Approach**

Our approach to achieving these goals is informed and guided by a set of principles that reflect our values, beliefs, and priorities as a Nation. The guiding principles that define our approach include our ability to galvanize action within and beyond the Federal Government, and effectively manage risk by focusing our efforts on those enhancements that result in the most significant improvement or reduction in risk.
This Strategy is focused on those components of the worldwide network of transportation, postal and shipping pathways, assets, and infrastructures by which goods are moved until they reach an end consumer. This includes the points of manufacturing, assembly, consolidation, packaging, shipment, and warehousing as well as supporting communications infrastructure and systems.\(^3\)

**Galvanize Action**

In order to meet the challenge to strengthen the global supply chain we must promote integrated and collective action among all levels of government, the private sector, and other key stakeholders. As we work to achieve our strategic vision, we will seek to:

- **Integrate our Federal efforts** by finding smarter and more cost-effective ways to address security threats and maximizing resources and expertise from across the United States Government. We will work to improve initiatives throughout the Federal Government by developing similar requirements, streamlined processes, and enhancing our information-sharing practices.

- **Foster an all-of-nation approach** to leverage the critical roles played by state, local, tribal and territorial governments, and private sector partners in strengthening supply chains. We will manage seams between their activities and Federal efforts by empowering these stakeholders to contribute to the mission. This will also develop a culture of mutual interest and shared responsibility.

- **Think globally** by enhancing our coordination with the international community and foreign stakeholders who also have key supply chain roles and responsibilities. The global supply chain transcends national borders and Federal jurisdiction. In recognition of this, we will seek to develop and implement global standards, strengthen detection, interdiction, and information sharing capabilities, and promote end-to-end supply chain security efforts with the international community.

**Manage Supply Chain Risks**

The global supply chain is subject to an ever-evolving array of risks. Our competitiveness as a Nation depends on managing risks to supply chain-related physical infrastructures to enable the movement of goods, energy, people, and information from one place to another. To manage risks, we will work to:

- **Understand and address vulnerabilities** to the supply chain that stem from both exploitation of the system by those seeking to introduce harmful products or materials and disruptions from intentional attacks, accidents, or natural disasters. We will focus our efforts on those risks that can bring the most harm to American citizens or threaten the functionality of the supply chain system.

---

\(^3\) In particular, the Strategy is intended to address: cargo transported within the legitimate supply chain, including imports and exports; movement of U.S. military cargo by commercial conveyances; commercial transport modes (air, land, and sea), including the intermodal freight transportation system; and organizations, groups, or individuals who have, or otherwise control, or have direct access to cargo, infrastructure, or information associated with the supply chain.
• **Utilize layers of defense** to protect against a diverse range of traditional and asymmetric threats. These layers include: intelligence and information analysis; appropriate use of technology; our laws, regulations, and policies; properly trained and equipped personnel; and effective partnerships.

• **Adapt our security posture** to meet evolving threats. We will work to promote a dynamic and flexible risk management approach that prioritizes actions to address risks with the greatest potential impact. We must also establish an environment in which we assess emerging threats and reprioritize our actions accordingly.

**The Path Forward**

Implementation of this Strategy will begin immediately upon its release. In the near term, we will focus our efforts on priority action areas identified during the development of the Strategy. These include:

• Align Federal activities across the United States Government to the goals of the Strategy.

• Refine our understanding of the threats and risks associated with the global supply chain through updated assessments.

• Advance technology research, development, testing, and evaluation efforts aimed at improving our ability to secure cargo in air, land, and sea environments.

• Identify infrastructure projects to serve as models for the development of critical infrastructure resiliency best practices.

• Seek opportunities to incorporate global supply chain resiliency goals and objectives into the Federal infrastructure investment programs and project assessment process.

• Promote necessary legislation that supports Strategy implementation by Federal departments and agencies.

• Develop, in concert with industry and foreign governments, customized solutions to speed the flow of legitimate commerce in specific supply chains that meet designated criteria and can be considered low-risk.

• Align trusted trader program requirements across Federal agencies. We will consider the potential for standardized application procedures, enhanced information-sharing agreements, and security audits conducted by joint or cross-designated Federal teams.

We will also actively engage domestic and international partners to develop specific recommendations in addition to the Federal efforts discussed above, and chart a course forward for achieving them. We have established a formal process to solicit feedback from the range of stakeholders with missions and
interests in the global supply chain. The input received through this process will help develop and prioritize recommendations for out-year implementation of the Strategy. In particular, we will garner input from the private sector and state, local, tribal, and territorial partners through the Cross-Sector Supply Chain Working Group under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework. We will also work to solicit inputs from foreign governments and interested international organizations.

Departments and agencies will submit to the President, through the Assistant to the President for Homeland Security and Counterterrorism, a consolidated report on implementation status within 1 year of the release of the Strategy. This report will detail progress made on each of the priority action areas identified above. It will also include additional recommendations for future action developed during the outreach process.

**Conclusion**

The global supply chain system that we seek will support innovation and prosperity by expeditiously, securely, and reliably moving goods and services within our domestic borders and around the world. This Strategy stands as testimony to partners, as well as warning to adversaries, that our efforts to strengthen this vital system will continue. We will build upon the solid foundation of previous efforts but also look ahead to the future we are working to create. Our Strategy is therefore one of continuity and of change. The threat of natural disasters remains, and the global supply chain and its components continue to be attractive targets for terrorist attacks and criminal exploitation. And while the security of our citizens and our nation is the paramount concern, we must work to promote America’s future economic growth and international competitiveness by remaining open for businesses to the world.

---

4. The CIPAC is a Federal Advisory Committee Act-exempt body established by the Secretary of Homeland Security, as authorized in Section 871(a) of the Homeland Security Act [6 U.S.C. §451(a)], to implement the National Infrastructure Plan (NIPP) Framework. The NIPP Framework is a partnership between government and critical infrastructure and key resources owners and operators, and provides a forum in which they can engage in a broad spectrum of activities to support and coordinate critical infrastructure protections. For more information, please visit [http://www.dhs.gov/files/committees/editorial_0843.shtm](http://www.dhs.gov/files/committees/editorial_0843.shtm)
## Contents

Executive Summary ........................................................................................................................ 3  
Introduction ..................................................................................................................................... 7  
Implementation Accomplishments and Next Steps ................................................................. 8  
Understanding Supply Chain Threats and Risks ................................................................. 8  
Advancing Cargo and Supply Chain Technology ............................................................... 10  
Building Resilient Critical Infrastructures .............................................................................. 11  
Promoting Necessary Legislation ......................................................................................... 13  
Promoting the Development and Implementation of Supply Chain Standards .............. 15  
Improving Commercial Information Analysis and Sharing Capabilities ......................... 17  
Streamlining Processes and Developing Customized Solutions ......................................... 18  
Continuing Engagement with Stakeholders ......................................................................... 20  
Conclusion ................................................................................................................................. 21
Executive Summary

The National Strategy for Global Supply Chain Security (Strategy), released in January 2012, establishes the United States Government’s policy to strengthen the global supply chain to protect the welfare and interests of the American people and to enhance our Nation’s economic prosperity. The Strategy complements and supports existing policies, and emphasizes:

- All modes of transport (air, land, and sea) as well as critical intermodal hubs to provide “end-to-end” coverage of the supply chain system;
- An all-hazards approach, recognizing that man-made as well as natural threats could trigger disruptions to the system; and
- The need for the global supply chain system to be both more secure and able to recover quickly should an incident occur.

The primary focus during this first year of implementation has been to build additional models and assessments for how the global supply chain system operates as an interconnected network. Much of this work built upon existing analysis of the systems’ constituent parts and, as a result, the United States Government now has a greater ability to describe, predict, and mitigate the disruptions that could affect the different types of supply chains that feed our domestic critical infrastructures and contribute to our national welfare and economic prosperity. This is a necessary first step toward the ultimate goal of developing and institutionalizing global measures to enhance the security, efficiency, and resilience of this vital global system.

As required by the Strategy, this report summarizes progress made by Federal departments and agencies in strengthening the global supply chain system during the first year of implementation.1 It also highlights opportunities for continued work and makes recommendations for future implementation activities.

2012 Accomplishments

Over the last year, the United States Government made good progress in advancing the priority actions identified in the Strategy’s Implementation Guidance. These priority actions include:

- Refining our understanding of supply chain threats and risks by completing insightful new assessments of the system as an interconnected network and updating analysis of the

---

1 The Strategy for Global Supply Chain Security notes that “Departments and agencies will submit to the President, through the Assistant to the President for Homeland Security and Counterterrorism, a consolidated report on implementation status within 1 year of the release of the Strategy. The report will detail progress made on each of the priority action areas identified [in the Strategy]. It will also include additional recommendations for future action developed during the outreach process.”
specific radiological or nuclear terrorist threat that reaffirmed current policies and programs.

- Advancing technology by establishing United States Government priorities in the supply chain space (such as tracking and intrusion detection capabilities for containers in transit) and developing a process to better coordinate research and development projects to advance those priorities; and supporting international capabilities to identify the illicit transport of radiological and nuclear materials in the supply chain by increasing the number of detection systems provided to foreign government partners.

- Building resilient critical infrastructures by creating new incentives, such as Resilience STAR, to encourage industry stakeholders to build resilience into their supply chains, which then strengthens the system overall; mapping the interdependencies among the supply chains of various critical infrastructure sectors (such as energy, cyber, and transportation); and creating common resilience metrics and standards for worldwide use and implementation.

- Promoting the development and utilization of supply chain standards through active engagement with relevant stakeholders to advance technical standards for radiation and nuclear detection technologies as well as global standards or best practices guiding the submission and analysis of postal and air cargo information.

- Improving commercial information analysis and sharing capabilities through innovative pilots with foreign governments to assess data and inspect high-risk cargo prior to arrival at the U.S. border.

- Streamlining and harmonizing government processes and policies to facilitate trade by completing milestone mutual recognition arrangements with the European Union for air, land, and sea cargo security programs; establishing four virtual Centers of Excellence and Expertise to improve the uniformity of trade enforcement processes among all our Nation’s ports of entry; and creating a new Interagency Trade Enforcement Center to identify and address unfair trade practices.

- Establishing a Cross Sector Supply Chain Working Group, composed of private sector representatives from domestic critical infrastructure sectors, and supporting their development of a “Global Supply Chain Findings and Recommendations Report” that will inform future implementation efforts.

2013 Implementation Activities

---

2 The 2012 arrangement with the European Union brings the total number of mutual recognition arrangements to seven Customs Trade Partnership Against Terrorism and Authorized Economic Operator mutual recognition arrangements; a maritime security mutual recognition arrangement with the European Union, air cargo security mutual recognition arrangements with 33 foreign nations, and mail security requirements with 32 nations.
Throughout 2012, Federal departments and agencies engaged with industry, international organizations, and other government stakeholders to identify areas for focus in 2013. These 2013 implementation activities include:

- Continuing to refine the United States Government’s understanding of threats and risks to the global supply chain system as an interconnected network by exchanging views on threats and risk with key domestic and international stakeholders, and advancing long term efforts to characterize system-wide risk and develop common risk indicators, metrics, and mitigation measures.

- Further aligning technology needs and investments among Federal departments and agencies by developing a set of United States Government-wide cargo and supply chain research and development (R&D) priorities; and identifying opportunities to test, in operational environments, specific technologies that have the potential to improve the security and integrity of cargo.

- Supporting international capabilities to detect and address the illicit global transport of radiological and nuclear materials and devices and other prohibited items and contraband.

- Promoting supply chain and critical infrastructure resilience by designating new Resilience STAR projects in the transportation sector; conducting exercises to identify and address critical infrastructure dependencies; and utilizing lessons learned from Hurricane Sandy to inform new policies and programs that will enhance our Nation’s preparedness.

- Engaging Congress to identify opportunities to enhance alignment between legislative requirements and the goals and approach established by the Strategy.

- Advancing selected global supply chain standards by strengthening intragovernmental coordination to better convey a unified, “whole-of-government” position during engagements with standards development or other intergovernmental organizations and bilaterally with foreign governments.

- Improving information sharing among Federal departments and agencies and with the private sector by establishing a task force to accelerate implementation of key components of the International Trade Data System; and by formalizing information-sharing agreements where necessary to improve the United States Government’s situational awareness of cargo and goods moving throughout the supply chain system.

- Streamlining and integrating public-private partnership programs requirements across relevant Federal departments and agencies and with key foreign trading partners.

- Emphasizing the completion of additional mutual recognition arrangements with key trading partners.
Engaging industry stakeholders and private sector owners and operators by continuing the Cross Sector Supply Chain Working Group, and increasing the coordination and awareness between it and other industry or government advisory groups.
Introduction

Securing the global supply chain system is integral to securing both the lives of people around the world and maintaining the stability of the global economy. The very nature of travel and trade in our networked world means that a disruption – whether natural, accidental, or malicious – in one part of the chain can have major implications thousands of miles away. Beyond loss of life and physical damage, these events can cause considerable economic consequences.

The *National Strategy for Global Supply Chain Security* establishes a government-wide vision of our goals, approach, and priorities to strengthen the global supply chain system. The Strategy establishes two explicit goals: promoting the efficient and secure movement of legitimate goods and fostering a global supply chain system that is resilient to natural as well as man-made disruptions. The Strategy also establishes the approach the United States Government will rely upon to achieve these goals – namely risk management and coordinated engagement with key stakeholders who also have key supply chain roles and responsibilities. In particular, the Strategy focuses on the worldwide network of transportation pathways, assets, and infrastructure (including supporting communications systems) by which goods are moved from the point of manufacture until they reach an end consumer.

The underlying goals and approach found in the Global Supply Chain Strategy not only reflect the President’s policy, as found in the National Security Strategy, but are hallmarks of other activities being advanced by the Administration. These other related activities include: enhancing cyber-security; improving critical infrastructure security and resilience; combating transnational organized crime; building our national preparedness capabilities; and enhancing the public health and safety of the American people.

As a result of the Strategy and implementation efforts throughout this first year, the United States Government has developed additional models and assessments to better understand how the global supply chain system operates as an interconnected network. These new insights have enhanced our ability to prevent, protect against, respond to, and recover from national level or system-wide supply chain disruptions and exploitations of the network.

Much of this work builds upon existing analysis of individual supply chain components, to include the different sectors and the facilities, transportation conveyances, and even processes involved in manufacturing goods and moving them to their final destination. The purpose of the Strategy was not simply to add to this volume. Instead, the Strategy provided, and will continue to provide, a framework to support the United States Government’s efforts to identify cross-cutting trends, priorities, and needs across all supply chain sectors and components and use this information to develop a more strategic approach to strengthening the system overall.
Implementation Accomplishments and Next Steps

The United States Government focused immediate Strategy implementation on specific priority actions grouped within several broad topic areas, to include:

- Refining the United States Government’s understanding of supply chain threats and risks;
- Advancing technology;
- Building resilient critical infrastructures;
- Identifying and promoting necessary legislation;
- Promoting the development and implementation of priority supply chain standards;
- Improving commercial information analysis and sharing capabilities;
- Streamlining and harmonizing processes and policies and developing customized solutions;
- Continuing engagement with industry partners, critical infrastructure owners and operators, and other stakeholders.

Simultaneously, Federal departments and agencies engaged with industry, international organizations, and other government stakeholders to determine additional areas for longer-term attention. This report summarizes the accomplishments achieved during this first year of implementation, and key activities identified during the engagement period that will be the focus of 2013 implementation efforts within each of the previously noted topic areas.

Understanding Supply Chain Threats and Risks

The Strategy establishes risk management as one of the key guiding principles of our approach to promoting a secure, safe, efficient, and resilient supply chain system. The first step to effective risk management is to identify and understand risks across the system as a whole. The evolving and dynamic nature of threats and vulnerabilities make this a challenging task, complicated further by the scope and complexity of the system itself.

Key Accomplishments To Date

Strategy implementation efforts in 2012 evolved the United States Government’s understanding of supply chain threats and risks through the following initiatives:

- **Assessing Threats to the Global Supply Chain System.** The Office of the Director of National Intelligence coordinated the development of an Intelligence Community Assessment (ICA) of Threats to the Global Supply Chain System. The ICA, completed in December 2012, represents the first-ever United States Government assessment of the range of known threats that could trigger national or network-level disruptions to the supply chain system and impact the United States’ interests both at home and abroad.\(^3\) The assessment was

\(^3\) The ICA is distinct from current assessments that consider the threats associated only with the supply chains of specific critical infrastructure sectors (such as manufacturing, transportation, energy, banking and finance, etc.). It is also distinct from existing assessments that consider the threats presented by the supply chain system itself (for
novel in its consideration of the global supply chain as an interconnected system of systems, and on how potential disruptions might impact its functioning directly, rather than viewing it from the point of its potential to be misused to deliver threats to other infrastructure. The ICA provides a common perspective of the global supply chain system threat environment to inform current and future efforts across the United States Government that have a supply chain nexus.

- **Combating Radiological and Nuclear Terrorism.** The Department of Homeland Security’s (DHS) Domestic Nuclear Detection Office (DNDO) and relevant departments and agencies conducted a radiological and nuclear terrorism risk assessment that addressed two areas: 1) the balance of risk across different transit modes and pathways within the global supply chain and 2) the balance of risk between supply chain and non-supply chain pathways. The analysis examined global supply chain pathways (air, land and sea) initiating at foreign ports of departure, continuing through the domestic ports of entry and concluding at potential targets. The assessment reaffirmed the necessity of a layered and risk-informed approach to protect the Nation from the threat of nuclear terrorism.

- **Initiation of a Longer-Term Effort to Characterize Global Supply Chain Risk.** Work during 2012 focused on developing a United States Government characterization of major disruptions to the transportation elements of supply chains, a first step toward the development of a comprehensive “end to end,” cross-sector, threat-neutral supply chain risk assessment. The risk characterization effort concluded that while major disruptions (characterized as events causing economic consequences over $100 billion in a single event or annualized) to the global supply chain are unlikely, a wide range of threat/hazard and vulnerability pairings (such as natural disasters, intentional attacks, and cyber events) could have dramatic impacts.

**2013 Priority Implementation Activities**

In 2013, Federal departments and agencies will work to implement five supply chain threat and risk priorities, including:

1. Refine and utilize risk assessments, such as the Radiological/Nuclear Global Supply Chain Risk Assessment, to inform the deployment of technical solutions and other capabilities internationally and domestically to strengthen the Global Nuclear Detection Architecture and related national policies and programs.

2. Advance efforts to characterize likely Radiological/Nuclear material and devices, including sensitivity, size, and weight of the expected device or material, and their potential transport pathways.

---

example, as a means to introduce illicit items such as weapons of mass destruction related materials, counterfeit, contaminated, or illegal goods) into the Nation hidden amongst legitimate shipments).
3. Develop and institutionalize a process to characterize and assess system-wide risk in coordination with industry and foreign government stakeholders globally. Specific areas for follow on work include:
   - Analyzing the balance of different risks to the global supply chain (such as the risk of small scale but frequent disruptions that may have a considerable cumulative impact and less frequent but more significant disruptions);
   - Identifying triggers that could cause small or localized disruptions to escalate;
   - Analyzing the exchange points in the supply chain, when goods are transitioned between different modes (from vessel to rail, for example); and
   - Developing and launching a global partnership on supply chain risk and resilience, through continued engagement with the private sector and foreign governments, both bilaterally and through multilateral organizations such as the World Customs Organization (WCO), the International Civil Aviation Organization (ICAO), and the International Maritime Organization (IMO).

4. Assess cyber security related risks to DHS systems used to collect, maintain, and analyze commercial data as well as systems operated on behalf of DHS necessary to secure the exchange of this data among private and public stakeholders.

5. Maintain a repository of global supply chain threat reporting and assessments to support future analysis as well as periodic updates to the ICA on Threats to the Global Supply Chain.

**Advancing Cargo and Supply Chain Technology**

Effective coordination and use of capabilities across Federal agencies, and with other stakeholders, is critical in this resource constrained environment in order to respond to evolving threats. This is particularly important for technology investments, as these systems are costly and time-consuming to implement.

**Key Accomplishments To Date**

Cargo and supply chain technology Strategy implementation efforts in 2012 focused on:

- **Assessing Currently Available Technologies.** DHS coordinated the development of a government-wide baseline assessment of currently available cargo and supply chain related technologies used or approved for use by the United States Government. The assessment highlighted: the need for integrated or cross-functional systems to address multiple threats; improved mobile detection capabilities to secure goods in transit; improved technologies to inspect rail cars and non-containerized cargo; the recent implementation of new technology to detect counterfeit and adulterated products; and enhancements to data management and automated targeting systems.

- **Supporting International Detection Capabilities.** Federal departments and agencies worked in collaboration with foreign government partners to enhance global capabilities to identify
the illicit transport of radiological and nuclear materials in the supply chain by increasing the international deployments of sensor systems and other detection equipment.

- **Prioritizing Research and Development Needs.** Federal departments and agencies identified research and development projects that would improve the security of goods in transit through the global supply chain system (to include tracking and intrusion detection capabilities for goods, containers, and conveyances as well as non-intrusive inspection systems) and developed a process to better coordinate United States Government efforts to advance those projects. This effort also highlighted the need for a mechanism to better integrate R&D efforts with system acquisition programs.

**2013 Priority Implementation Activities**

In 2013, Federal departments and agencies will work to implement two supply chain technology priorities, to include:

1. Develop a United States Government-wide Cargo and Supply Chain R&D Plan to align technology needs with investments, including planning for future security hardware and systems upgrading.

2. Advance technologies that improve the security and integrity of goods in transit, such as radiological and nuclear detection and identification systems as well as container security devices, locks, seals, or tracking mechanisms, from R&D into operational environments, in coordination with industry stakeholders. Conduct a pilot program, in concert with interested foreign governments and industry partners, to assess the capability of promising prototype supply chain technologies (such as the “hybrid security shipping container”) in an appropriate trade route in the supply chain system.

**Building Resilient Critical Infrastructures**

Recognizing that a variety of man-made and natural incidents have the potential to severely disrupt normal commerce, the Strategy emphasized the need to foster a global supply chain system that can adapt to changing conditions and withstand and rapidly recover from disruption. There are a number of resilience efforts underway currently focused on specific threats or critical infrastructure sectors, such as efforts to enhance individual and community resilience or to develop information technology systems and electricity and energy supply chains that are resilient to cyber threats or other disruptions.

**Key Accomplishments To-Date**

---

‘Non-intrusive cargo inspection technologies’ refers to those technologies which allow an inspection to be performed from the outside the container or conveyance without having to break containment and/or not requiring entry.
Implementation activities in 2012 focused on enhancing the resilience of the global supply chain as a comprehensive and networked system, including:

- **Advancing the Institutionalization of Resilience Methods and Metrics.** Building on previous work with the private sector and multilateral organizations such as the World Customs Organization and the Asia-Pacific Economic Cooperation (APEC), Federal departments and agencies developed global guidelines on information sharing for transportation system disruption. In addition, the United States Government engaged with and supported the efforts of organizations such as the World Economic Forum to highlight the need for common definitions, metrics, and standards for supply chain resilience.

- **Encourage implementation of resilience practices.** The Department of Transportation (DOT) and DHS identified ongoing, domestic transportation infrastructure projects where asset owners and operators are incorporating resilience best practices into their design and construction. These projects, which included bridges, tunnels, maritime ports, and rail systems, will inform the development of national as well as global resilience metrics.

- **Understanding the Interdependencies of Critical Infrastructures and Supply Chains.** The Federal Emergency Management Agency (FEMA) identified potential vulnerabilities to critical infrastructures and key supply chains during several table-top exercises with private sector stakeholders throughout the Mid-Atlantic region of the United States. The findings of these exercises, in which critical infrastructure dependencies were identified through simulated events designed to stress the supply chain system, will inform both public and private efforts to enhance mitigation, preparedness, response, and recovery capabilities at both the local and regional level. For example, efforts associated with this project led to the identification of a variety of private sector resources capable of providing shared real-time operational information on supply chain disruptions during the response to Hurricane Sandy in 2012. Many of these resources had not been used for this purpose before, but provided valuable insight into how to deploy resources better in order to support supply chain restoration.

- **Ensuring Medical Countermeasure Supply During a Public Health Emergency.** The U.S. Department of Health and Human Services (HHS) created a new capability on June 15, 2012, by awarding contracts to three Centers for Innovation in Advanced Development and Manufacturing based in Maryland, North Carolina, and Texas. Together the Centers will expand the nation’s domestic ability to respond to bioterrorism threats, pandemic influenza, and other epidemics. These Centers offer a new model for public-private partnerships, bringing together small biotech companies, academic institutions and large experienced pharmaceutical companies to develop and deliver medical countermeasures quickly and cost effectively.

**2013 Priority Implementation Activities**
In 2013, Federal departments and agencies will work to implement five supply chain resilience priorities:

1. Expand the Resilience STAR Program into the transportation sector and seek additional opportunities to highlight good resilience practices.\(^5\)

2. Advance the development of resilience metrics and standards that will allow stakeholders to better assess the value and performance of their efforts to incorporate resilience into their supply chains and provide a means to measure the resilience of specific critical infrastructure sectors as well as the system overall.

3. Highlight resilience improvements by providing information on Federal websites for both domestic and international stakeholders.

4. Conduct follow-on studies and exercises, building on the progress of the 2012 FEMA regional project, with an expanding number of private sector participants and a broader geographic range. Also, collaborate with private sector partners to further assess opportunities to utilize industry situational awareness tools identified during the response to Hurricane Sandy to be more effectively utilized in response, restoration, and recovery of supply chains.

5. Ensuring medical countermeasure supply during a public health emergency. HHS expects to release a request for proposals in early 2013 to establish a network of biopharmaceutical ‘fill and finish’ manufacturers. This U.S. based network of facilities is expected to collectively provide filling and finishing manufacturing capabilities for influenza vaccines and other public health products to address national security and to augment public health needs on a cost-effective, reliable, and sustainable basis.

**Promoting Necessary Legislation**

Federal departments and agencies regularly engage with Congress to develop legislative solutions to allow or enhance their ability to secure the supply chain system while promoting efficiencies and reducing costs.

**Key Accomplishments To Date**

\(^5\) The Resilience STAR program is a private-public partnership that seeks to enhance resilience across national critical infrastructure sectors by providing measurable, industry-approved performance targets which owners and operators voluntarily can meet in order to receive a “STAR” certification. Inspired by certification systems such as ENERGY STAR and the Leadership in Energy and Environmental Design (LEED), Resilience STAR seeks to provide a similar market differentiator for the concept of resilience against significant disasters, be they natural or man-made.
Strategy implementation efforts in 2012 focused on the following activities:

- **Securing Maritime Cargo.** DHS, in coordination with other relevant Federal departments and agencies, worked to identify potential alternatives to the “100 percent maritime scanning” provision (Section 232 of the Security and Accountability for Every (SAFE) Port Act of 2006, as amended) that would focus threat mitigation efforts on high risk shipments. DHS has exercised its statutory authorities to extend the 2012 implementation deadline. DHS and other relevant Federal departments and agencies have determined, however, that significant challenges will likely preclude full implementation of the provision in the specific manner prescribed. Therefore, DHS considered alternative approaches to secure the maritime pathway against the threat of nuclear terrorism that aligned with the United States Government’s Global Nuclear Detection Architecture and other relevant programs and policies, and that was consistent with international trade obligations and global standards promulgated by the World Customs Organization. DHS will use these potential alternatives to inform continued engagement with Congress on the issue.

- **Strengthening Drug Supply Chains.** The Food and Drug Administration (FDA) has worked to implement requirements under the 2012 Safety and Innovation Act (FDASIA), including drug supply chain safety provisions, such as requirements for the FDA to establish a unique facility identifier for each establishment registered with the FDA.

**2013 Priority Implementation Activities**

In 2013, Federal departments and agencies will work with the Congress and others to address four supply chain priorities in the legislative and regulatory environment, to include:

1. **Engage Congress to identify opportunities to enhance alignment between legislative requirements associated with the use of sensor based radiological and nuclear technologies abroad and the goals and approach established by the Strategy, the Global Nuclear Detection Architecture International Implementation Plan, and other relevant programs and policies.**

2. **Continue to advance cooperation with foreign governments, such as the United States-Canada Regulatory Council and Beyond the Border Initiative and the United States-European Union Transnational Economic Council, with a focus on enhancing global supply chain security, safety, efficiency, and resilience.**

3. **Expand DHS authority to share information with rights holders to ascertain whether imported and exported goods violated intellectual property laws.**

4. **Consider options, including legislative, to authorize agencies to disclose confidential business information to Federal, state and local law enforcement authorities under certain circumstances.**
Promoting the Development and Implementation of Supply Chain Standards

Today’s supply chain systems transcend national borders and geographic regions and involve a number of private and public sector stakeholders. Global standards, best practices, and guidelines provide a common framework by reducing compliance burdens for industry, allowing governments to realize efficiencies, and maintaining acceptable levels of security. The United States Government will continue to work with intergovernmental bodies and standard-development organizations to develop and implement global standards for technologies, management policies, training protocols, and other supply chain related issues.6

Key Accomplishments To Date

The United States Government focused 2012 Strategy implementation on the following standards related activities:

- **Advancing the Secure Supply Chain Initiative.** DHS, on behalf of the United States Government, sought to strengthen ties among, and advance a common agenda with, supply chain-related multilateral organizations.7 This initiative, which began in 2011 and continued throughout 2012, was successful in advancing several priority global supply chain standards and best practices. For example, it resulted in new reporting requirements associated with the transport of certain improvised explosive device precursor materials and the development of a common definition for high risk cargo between customs and law enforcement agencies.

- **Strengthening International Mail Standards.** The United States Government, in concert with foreign government and industry partners, secured the passage of several key resolutions to improve international postal supply chain security by the Universal Postal Union (UPU) during the quadrennial Congress convened in Doha, Qatar, in October 2012. These key provisions involved global standards for advance data on mail shipments for security purposes as well as standard processes for responding to and resolving anomalies detected at international transit hubs. The 192 member nations of the UPU will work to implement these changes in 2013.

- **Strengthening Global Air Cargo.** The United States Government made considerable progress in 2012 to strengthen requirements associated with commerce transported on passenger and all-cargo aircraft. These efforts included achieving, in collaboration with

---

6 Where any international regulatory cooperation activities are reasonably anticipated to lead to significant regulatory actions, agencies conduct their work in a manner consistent with Executive Order 13609 (“Promoting International Regulatory Cooperation).

7 These multilateral bodies include the WCO, the ICAO, the IMO, the APEC, the UPU, and the International Atomic Energy Agency (IAEA).
industry stakeholders, 100-percent screening of air cargo transported on passenger aircraft destined to the United States. Federal departments and agencies also worked collaboratively with foreign government and private sector stakeholders to assess the feasibility and benefits of industry submission of key data associated with goods prior to an aircraft’s departure from a foreign location. In addition, the United States Government encouraged the first ever joint WCO and ICAO working group on air cargo to develop guidelines for advance information requirements that would meet both customs and law enforcement needs. These efforts will support the development and implementation of global air cargo information standards and guidelines, resulting in streamlined processes for industry stakeholders and improved targeting capabilities for governments.

- Improving Intra-Government Coordination on Standards Development and Implementation. In 2012, Federal departments and agencies assessed current processes within the United States Government for developing and using relevant international standards associated with select global supply chain issues and identified opportunities for improvement. Some of these suggested improvements are being discussed in the context of ongoing work to update Office of Management and Budget (OMB) guidance to Federal departments and agencies participating in the development and use of voluntary consensus standards to better advance “whole of government” positions. In addition, the assessment identified nine specific supply chain standards, guidelines, or best practices whose advancement would benefit from enhanced coordination among Federal departments and agencies and more active United States Government engagement overall. These key standards, guidelines, and best practices range from standards governing the use of privately contracted armed security personnel on board ships to combat piracy, technical standards for detection equipment, and comprehensive supply chain management standards designed to help stakeholders understand the network as a whole and better manage the movement of their goods within it.

2013 Priority Implementation Activities

In 2013, Federal departments and agencies will work to advance four standards development activities related to global supply chain topics, including:

1. Advance the development and implementation of key global supply chain related standards, best practices, and guidelines to advance goals established by the Strategy, through appropriate multilateral organizations, standards developing organizations, and bilaterally with key trading partners. As part of this effort, Federal departments and agencies will track participation in these organizations, either through established mechanisms or through the development of new policies and procedures, to enhance internal United States Government coordination and better convey a “whole of government” perspective. This effort will also continue to explore mechanisms to encourage stakeholder adoption of global standards, best practices, and guidelines.

---

8 OMB Circular A-119.
2. Enhance or develop guidelines and training within Federal departments and agencies for employees engaged in standards or guidelines development to increase the strategic effectiveness of Federal engagement in standardization processes in order to advance national goals.

3. Evaluate the pros and cons of a formalized process to coordinate U.S. positions on appropriate efforts at the international level so as to ensure a coherent U.S. approach and/or to track participation in standards development in the supply chain space and share relevant information with stakeholders.

4. Initiate rulemaking for air cargo advance information requirements informed by ongoing pilot operations and continued coordination with stakeholders.

Improving Commercial Information Analysis and Sharing Capabilities

The United States Government relies upon the collection, analysis, and sharing of commercial and associated supply chain information with industry stakeholders to enforce compliance with laws and regulations and to identify shipments that warrant additional scrutiny. Strategy implementation efforts in 2012 sought to advance both critical ongoing initiatives, such as the International Trade Data System (ITDS), as well as more recent efforts to refine advance data requirements to strengthen targeting capabilities and facilitate legitimate commerce.

Key Accomplishments To Date

Specific information sharing and analysis accomplishments in 2012 included:

- **Establishing ITDS implementation as a critical national-level priority.** A total of 47 agencies are working together on the ITDS program. Through ITDS, the Automated Commercial Environment (ACE) will become the “single window” system, intended to eliminate redundant reporting requirements and speed cargo processing by collecting commercial data from industry and distributing it electronically to the appropriate regulatory or law enforcement agency. The potential longer-term cost savings of ITDS are considerable. Implementation of ITDS has been complicated by technical and operational challenges, funding constraints, and unclear schedules associated with the delivery of key capabilities. DHS, which is responsible for operating and maintaining ITDS, and the Department of the Treasury, which serves as interagency coordinator, and other participating government agencies have worked together to identify specific opportunities to raise awareness of this critical effort, speed development of key functionality, and resolve outstanding policy and regulatory issues to achieve government-wide implementation as soon as possible.

---

9 Agencies with licensing and compliance responsibilities are required to join ITDS by the SAFE Port Act of 2006 and by OMB Memorandum M-07-23, September, 10, 2007 based on the recommendations of the President’s Working Group on Import Safety.
Working to advance these opportunities will be the 2013 priority, coordinated by an Administration Task Force (to include, as necessary, the National Security Staff, Office of Science and Technology, and OMB) and supported by the ITDS Board of Directors, the Border Interagency Executive Council and relevant Federal departments and agencies.

2013 Priority Implementation Activities

In 2013, Federal departments and agencies will work to advance two supply chain priorities related to information-sharing, including:

1. The ITDS Task Force will coordinate a range of activities, such as:
   • Finalize a long-term schedule and a shared understanding of ITDS capability development and availability by the first quarter of 2013;
   • Promote ITDS implementation by assessing the long term cost savings and other benefits of ITDS utilization and developing a common message for use by relevant Federal departments and agencies in their communications with external stakeholders.
   • Improve information sharing between Federal departments and agencies participating in ITDS by: revising regulations to allow for the collection and sharing of electronic (rather than paper-based) data; finalizing the remaining data-sharing agreements between agencies (a pre-requisite for information sharing); and, updating relevant Paperwork Reduction Act public notices and information collection approvals as necessary.
   • Develop and deploy 1-3 pilots to test the feasibility and benefits of enhanced technical interfaces and other exchanges between Federal departments and agency data collection systems and existing commercial targeting systems (such as DHS’ Automated Targeting System).

2. Formalize information-sharing arrangements between Federal agencies focused on cargo arriving and departing the United States, including law enforcement entities operating in the joint National Targeting Center for Cargo, and those agencies such as the Office of Naval Intelligence focused upon cargo moving between foreign ports to foster information sharing and analytic cooperation allowable under law.10

Streamlining Processes and Developing Customized Solutions

Strategy implementation efforts in 2012 focused on assessing ways to simplify and streamline existing programs and identify new opportunities to expedite trade through specific supply chains that meet robust, pre-established criteria.

Key Accomplishments To Date

---

10 The joint National Targeting Center for Cargo and the Office of Naval Intelligence have agreed to document formally their current mutual support practices and future opportunities for improved cooperation.
• **Simplifying and Strengthening Public-Private Cooperative Requirements.** The United States Government has developed a range of programs that leverage industry expertise and interests by facilitating the release of cargo for companies meeting specific criteria and maintaining solid compliance track records. Federal departments and agencies completed a comprehensive baseline assessment of existing public-private programs across the government that identified specific opportunities to enhance efficiencies and reduce costs associated with these programs. The assessment concluded that enhanced harmonization of Federal requirements could improve those public-private partnership programs focused on both supply chain security as well as efficiency (such as the Customs Trade Partnership Against Terrorism (C-TPAT) and the Importer Self-Assessment (ISA)).

• **Transforming Trade Enforcement Processes.** Federal departments and agencies enforce compliance with a variety of laws and regulations to ensure that goods entering and exiting our nation are safe, secure, legitimate, and meet our fair trade obligations. Significant progress was made in 2012 to consolidate these compliance functions where possible and to pilot new and innovative processes to expedite the release of highly compliant cargo. Examples include, DHS’ Simplified Entry concept, piloted in 2012 in the air environment, which gives industry stakeholders enhanced flexibility in providing required commercial data to government regulators and law enforcement. Another key accomplishment was the establishment by DHS of four Centers of Excellence and Expertise.\(^{11}\) Each of these strategic virtual centers brings DHS’s trade expertise to bear on a specific industry, providing tailored support to increase uniform requirements across ports of entry and facilitate the timely resolution of compliance issues nationwide.

• **Leveraging Intergovernmental Relationships.** The United States’ overall vision and collaborative approach to strengthening the global supply chain in partnership with other foreign governments is highlighted in the ongoing successful implementation of initiatives such as the United States-Canada Beyond the Border Initiative, and the 21st Century Border Management Initiative with Mexico. While these initiatives enhance bilateral cooperation across a range of issues, supply chain priorities are also well represented in work associated with facilitating legitimate trade and travel at the border, protecting key critical infrastructures, leveraging resources, and combating transnational organized crime. In addition, the United States Government enhanced engagement with the European Union in 2012 on supply chain and economic competitiveness issues and made significant progress with regional bodies such as the APEC and the Organization of American States.\(^{12}\) These intergovernmental partnerships, and relationships with multilateral organizations, underscore our commitment to develop collaborative solutions that simultaneously streamline procedures for customs processing and regulatory compliance; align and

---

\(^{11}\) Current Centers of Excellence and Expertise include: the Center for Information Technology and Consumer Electronics; the Center for Pharmaceuticals, Heath and Chemicals; the Center for Automotive and Aerospace; and the Center for Petroleum Natural Gas and Minerals. DHS anticipates establishing five additional Centers in 2013.

\(^{12}\) Specific achievements include approval and early implementation within the APEC forum of the Counterterrorism and Secure Trade Strategy as well as the initiation, within the Organization of American States, of a supply chain security program that will inform longer term work.
mutually recognize security and safety programs; and create opportunities to modernize infrastructure and expand the mutual capacity for trade.

2013 Priority Implementation Activities

In 2013, Federal departments and agencies will work to implement three activities to streamline processes and encourage customized solutions to strengthen the global supply chain system. These activities include:

1. Develop a “United States Government Supply Chain Partnership Program Framework” to inform Federal departments and agencies as they work to develop new supply chain partnership programs, or to refine existing ones to improve harmonization or achieve mutually recognition of requirements.

2. Develop and test centralized processing for applications and eligibility requirements for all U.S. global supply chain related partnership programs, where appropriate.

3. Solicit input from industry or other stakeholders on specific additional opportunities to streamline or enhance government operational processes associated with private-public supply chain partnership programs or to encourage additional stakeholder participation.

Continuing Engagement with Stakeholders

The majority of the global supply chain system is owned and operated by entities outside of the United States Government; industry must be empowered, through an “all-of-nation” approach, to contribute to enhancing security, efficiency, and resilience. In 2012, the United States Government focused implementation outreach efforts on soliciting input from foreign and domestic public and private sector partners to better understand their perspectives, needs, and priorities.

Key Accomplishments To-Date

- **Leveraging Industry Partnerships.** The Cross Sector Supply Chain Working Group served as the formal mechanism for public-private engagement on Strategy implementation. This group, operating under the Critical Infrastructure Partnership Advisory Council (CIPAC) model, included industry representatives from each of the critical infrastructure and key resource communities. After nearly 7 months of analysis and deliberation, the group

---

13 The CIPAC provides a legal framework and forum that enables members of the Sector Coordinating Councils and Government Coordinating Councils to engage in critical information and key resource joint protection-related discussions. The Secretary of the Department of Homeland Security exercises statutory authority created under the Homeland Security Act (P.L. 107-296) to exempt CIPAC meetings from the requirements of the Federal Advisory Committee Act (FACA). That exemption expressly establishes a known and trusted framework to uphold effective information sharing, risk mitigation of vulnerabilities; and use of necessary communications during emergencies.
submitted a “Findings and Recommendations Report,” detailing 11 recommendations for follow-on implementation work. Representatives from relevant Federal departments and agencies met with the group in late November and identified areas of mutual interest to advance collaboratively in 2013. These included:

- Continued public-private engagement to facilitate Strategy implementation;
- Joint exercises and planning activities to prepare for supply chain disruptions;
- Development and institutionalization of supply chain risk and resilience standards;
- Modernizing domestic critical infrastructure to improve capacity and promote economic competitiveness;
- Streamlining and simplifying government processes to facilitate commerce; and
- Strengthening public-private intelligence and information sharing policies and procedures.

2013 Priority Implementation Activities

In 2013, Federal departments and agencies will continue to engage industry partners and critical infrastructure owners and operators on the following activities:

1. Continue the Cross Sector Supply Chain Working Group, with any necessary updates to structure, management, and membership.

2. Increase collaboration and awareness between the Cross Sector Supply Chain Working Group and other industry or government advisory groups working to advance supply chain or critical infrastructure issues, including the Commercial Operations Advisory Committee, the Advisory Committee on Supply Chain Competitiveness, and National Maritime Security Advisory Committee, among others.

Conclusion

The economic prosperity of nations worldwide is dependent upon the supply chain system. No one in either the public or the private sector has the resources, the authorities or the full range of expertise to address this problem in isolation. Protecting the global supply chain is therefore, a shared responsibility. By understanding what needs to be done, we can together assess which stakeholder is best positioned – and has the tools and resources – to do it.

We have established a common vision with the National Strategy for Global Supply Chain Security to enhance collaboration among Federal departments and agencies and to also guide our interactions with key partners. As the United States Government continues to implement the Strategy and advance other related efforts, industry voices will remain critical to help inform the dialogue. We continue to rely upon Federal Advisory Committee Act process as well
as established mechanisms for private-public collaboration within and across the numerous
domestic critical infrastructure sectors (such as CIPAC).

The partnerships, and continued engagement with foreign governments, underscore our
commitment to developing collaborative solutions that simultaneously streamline procedures
for the processing of goods at borders; align and mutually recognize security programs; and
create opportunities to modernize infrastructure and expand capacity.
Private-Public (and Private-Private) Relationships emerging from Prospects of Catastrophic Risk

Philip J. Palin

Supply Chain Resilience
National Academy of Sciences
CNA Institute for Public Research
Rutgers University Graduate School
More Risk: Frequency

NatCatSERVICE
Loss events worldwide 1980 – 2013
Number of events

- Geophysical events (Earthquake, tsunami, volcanic eruption)
- Meteorological events (Tropical storm, extratropical storm, convective storm, local storm)
- Hydrological events (Flood, mass movement)
- Climatological events (Extreme temperature, drought, forest fire)

© 2014 Münchener Rückversicherungs-Gesellschaft, Geo Risks Research – As at January 2014
More Risk: Financial Cost
### Top 10 global business risks for 2014

<table>
<thead>
<tr>
<th>Rank</th>
<th>Risk Description</th>
<th>2014</th>
<th>2013</th>
<th>Rank</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Business interruption, supply chain risk</td>
<td>43%</td>
<td>46%</td>
<td>(1)</td>
<td>—</td>
</tr>
<tr>
<td>2</td>
<td>Natural catastrophes (for example, storm, flood, quake)</td>
<td>33%</td>
<td>44%</td>
<td>(2)</td>
<td>—</td>
</tr>
<tr>
<td>3</td>
<td>Fire, explosion</td>
<td>24%</td>
<td>31%</td>
<td>(3)</td>
<td>—</td>
</tr>
<tr>
<td>4</td>
<td>Changes in legislation and regulation</td>
<td>21%</td>
<td>17%</td>
<td>(4)</td>
<td>—</td>
</tr>
<tr>
<td>5</td>
<td>Market stagnation or decline</td>
<td>19%</td>
<td>12%</td>
<td>(8)</td>
<td>↑</td>
</tr>
<tr>
<td>6</td>
<td>Loss of reputation or brand value (for example, from social media)</td>
<td>15%</td>
<td>10%</td>
<td>(10)</td>
<td>↑</td>
</tr>
<tr>
<td>7</td>
<td>Intensified competition</td>
<td>14%</td>
<td>17%</td>
<td>(5)</td>
<td>↓</td>
</tr>
<tr>
<td>8</td>
<td>Cyber crime, IT failures, espionage</td>
<td>12%</td>
<td>(-)</td>
<td>(-)</td>
<td>NEW</td>
</tr>
<tr>
<td>9</td>
<td>Theft, fraud, corruption</td>
<td>10%</td>
<td>(-)</td>
<td>(-)</td>
<td>NEW</td>
</tr>
<tr>
<td>10</td>
<td>Quality deficiencies, serial defects</td>
<td>10%</td>
<td>13%</td>
<td>(6)</td>
<td>↓</td>
</tr>
</tbody>
</table>

The third annual Allianz Risk Barometer survey was conducted among risk consultants, underwriters, senior managers and claims experts in the corporate insurance segment of both Allianz Global Corporate & Specialty (AGCS) and local Allianz entities. Figures represent the number of responses as a percentage of all survey responses (557).
More Risk: Anticipated

March 2011
Tohoku Triple Disaster

Swiss Reinsurance company requires catastrophic analysis and mitigation by insurance carriers

German insurance carrier requires catastrophic analysis and mitigation by larger commercial clients

Anglo-Dutch holding company requires US grocery distribution company to deliver catastrophic analysis and mitigation plan

October 2011
Thai Floods

Grocery distribution company begins meeting with:

Electric Utilities
Retail Clients
Product Sources
Telecommunications Vendors
Third Party Logistics Providers
Local/State/Federal Emergency Managers
Others...
Problems Revealed

Vulnerability (and mitigation) emerge especially from system interdependencies

Most assume greater capability and capacity (by others) than usually exists

Competition and contending priorities complicate collaboration among private players

Cross-cultural issues between private and public

Tension between species-specific or ecosystem perspective
Opportunities Revealed

Risk “mutuality” is real, especially related to mitigation

**Mutuality is the principle of private, commercial insurance; individuals enter the pool for sharing losses, and pay according to the best estimate of the risk they bring with them.**

Opportunities Revealed
Emerging Legal Implications?

Force Majeure, Acts of God, Fortuitous event contract clauses anticipate catastrophes that are *outside the control* of the parties and *cannot be anticipated*.

**CONTROL**


**ANTICIPATION**

*General Construction Co Ltd v Chue Wing & Co Ltd* (Judicial Committee of the Privy Council, 2013): Cyclones are not uncommon, collapse of crane not protected under force majeure.
Emerging Legal Implications?

XVI
CONCLUSION

The application of a successful defense based on force majeure or Act of God necessarily focuses on human factors. The defense may be lost by a showing that actions of the party asserting the defense contributed to the casualty, or that notwithstanding acts of nature of exceptional magnitude, the loss could have been avoided by exercise of reasonable care, or adequate precautions. Mitigating factors and reasonableness of actions taken are also taken into account in decisions evaluating intervention of governmental authorities, acts of third parties, or other events beyond the control of the parties. While the careful practitioner will necessarily plead force majeure as an affirmative defense, the practical application of the doctrine is, essentially, a showing of due care, contingency planning and precautionary measures, lack of negligence, and reasonable conduct.

Gregory C. Buffalow
The Force Majeure Defense: Recent cases, Boilerplate and Analysis
Journal of Maritime Law and Commerce, April 2011
Supply Chain Resilience: 
Diversity + Self-organization = Adaptation 

Philip J. Palin 

ABSTRACT 
In the last three decades a collection of linear supply chains has become a complex adaptive network of demand creating supply. The benefits are obvious. The risks tend to be insidious. With the 2012 National Strategy for Global Supply Chain Security and the 2013 Implementation Update on the strategy, a public-private process has been engaged for considering risks and cultivating resilience. Complex adaptive systems are not well suited to traditional security mindsets. In the natural environment resilience emerges from diversity, self-organization, and innovation. Are these characteristics appropriate to the supply chain? Can these characteristics be systematically cultivated by private and public decision-makers who influence the supply chain? This essay points to prior examples of dealing with complex adaptive systems to suggest an affirmative conclusion. 

Supply has been unchained. Improvements in transportation – highways, fast high capacity planes, intermodal trains, trucks, and ships – combined with a revolution in computing and communications have transformed a dense lattice of overlapping chains of supply into a shared network for delivery-on-demand. 

Only thirty years ago a major retailer often owned most of the links in a chain that connected producer to consumer. No more. Almost everyone specializes in a horizontal or oblique or nodal niche. Each niche forms around functional expertise and comparative advantage. This global commons makes possible more goods at lower cost and with better assurance of quality than ever before. In the last generation we have experienced a rate of change and improvement in moving goods not equaled since steam-power transformed maritime shipping and made possible railroads. 

On June 26, 1974, at a Marsh supermarket in Ohio, a pack of Wrigley’s Juicy Fruit chewing gum became the first retail product sold using a scanner and Universal Product Code. The use of the UPC and other “bar codes” allows the supply chain to be digitally monitored, mapped, and managed as never before. Logistics has become one aspect of a constantly shifting supply and demand stream. 

Increasingly these processes – and the rich information and management resources they make possible – ensure effective, timely, and comparatively friction-free transactions between companies and nations. The ability to share digital information in very close to real-time has transformed the modern supply chain from supply-push to demand-pull. 

Farmers, miners, and fishermen still matter. Processors, truckers, wholesalers, and retailers still play crucial parts. Ports, railways, and highways are still required. Physical stuff of all sorts still has to move from point A to B (and usually on to points C, D, and Z). But at least in the United States, Europe, and Pacific Rim, the digital signals that are sent along largely determine when and where product arrives. 

When the strategic capacity for generating demand-pull information persists, the supply chain is very resilient. But disruption or corruption of this information stream also presents unprecedented challenges to supply, especially in crisis situations. In the aftermath of the March 11, 2011 earthquake-and-tsunami in Japan demand signals went dark across the hardest hit areas of Northeast Japan. At the same time, demand spiked in Tokyo and other
areas far from the impact zone. The supply chain responded adroitly to hoarding behavior by those whose demand could be communicated with a quick electronic scan. But this same behavior reduced the capability of Japanese producers and distributors to respond to the critical needs of those who had been rendered digitally mute.

Resulting in considerable United States comparative advantage

Source: Council of Supply Chain Management Professionals (2011)

Figure 1. Logistics as a Competitive Advantage
As late as 1980 the cost of logistics as a proportion of GDP was more than double what it is today. Over the last three decades logistics has become something very different than ever before.

For most of human history anticipating demand has been a guess. In a few cases, historical data might be used to project demand and some using it were better – or luckier – guessers than others. But mostly demand was met (or not) by producing and distributing what could be supplied at a price the producer hoped the market would pay. A nineteenth century economic doctrine, as stated by John Maynard Keynes, was “Supply creates its own demand.” Certainly true until the 1980s was supply creates its own distribution – in search of demand.

For most of human history inventory has equaled wealth. In the 1950s the president of Toyota declared that inventory is waste. Taiichi Ohno said, “The more inventory a company has, the less likely they will have what they need.” Toyota was a pioneer in what came to be called Just-In-Time manufacturing. To be effective, Just-In-Time (JIT) depends on a deep understanding of demand. Making and delivering where and when demand is expressed eliminates “waste” and increases profits. By focusing on customer needs and wants business can transition from “selling supply” to “serving demand.”

The competitive success of Toyota and other Japanese firms in the 1970s and ‘80s converted many US and other manufacturers to similar philosophies and practices. In 1983, Zero Inventories by Robert Hall articulated the ultimate goal and a workable process for achieving the goal. It was a process aided and abetted by the increasing ability of computer databases to store and analyze customer data.

In 1972 Walmart had fifty-one stores. By 1980 it had grown to 276 stores. In 1983 Walmart replaced all of its cash registers with computerized point-of-sale systems. In 1987 Walmart installed the largest privately owned satellite system in the United States to facilitate the increasing amount of demand and sales data being generated. In 1990 Walmart overtook Sears to become the nation’s largest retailer. In 1993, with nearly 2,000 stores, Walmart achieved its first billion dollar sales week. Today Walmart has nearly 10,000 stores and generates annual sales of over $422 billion. In terms of operating revenue it is the world’s largest private enterprise.

There are many explanations for Walmart’s phenomenal success, but according to a study by the University of San Francisco “Walmart owes its transition from regional retailer to global powerhouse largely to changes in and effective management of its supply chain.” The same study reports:

Technology plays a key role in Walmart’s supply chain, serving as the foundation of their supply chain. Walmart has the largest information technology infrastructure of any private company in the world. Its state-of-the-art technology and network design allow Walmart to accurately forecast demand, track and predict inventory levels, create highly efficient transportation routes, and manage customer relationships and service response logistics.

According to JIT guru Richard Schonberger, this technological capability is a very tangible expression of an even more important comparative advantage. Schonberger writes, “Wal-Mart is the world’s grand champion of lean supply chains. While advanced IT gets most of the credit, collaboration is the foundation. Wal-Mart’s 2,000-odd suppliers near the retailer’s Bentonville, Ark., headquarters maintain multifunctional teams on site.”

Streamlining and upgrading sources of supply has been fundamental to driving down costs across a wide array of supply chains. This was at the core of restructuring the American supply chain in the last two decades of the twentieth century. An example from the early 1980s:

Unisys, of New Jersey, cut its supplier base from 750 to 106 and reduced the number of trucking companies from 120 to 8. As a result, purchase costs have dropped by 40 percent, freight costs have been reduced from $.32 per pound to $.09 per pound, and transit times from...
the Far East have been cut by two-thirds.  

Success stories like this, and increased competition by early-moving innovators, transformed many product categories from supply-push to demand-pull. In 2000, the Department of Defense opened the Global Positioning System (GPS) to public use. This transformed the potential of trucks, in particular, to respond to irregular demand as effectively as was once only possible for most favored customers. Demand increasingly determined supply. In a period of barely three decades, technological innovations have radically transformed 5000 years of transportation history.

The results have also included increasing concentration, greater interdependence, and lower profit margins (even as gross profits have increased due to much higher volume). The supply chain at large – and individual supply chains – increasingly involves a complex set of inputs, outputs, and multi-layered relationships. And as with other complex entities, the supply chain can sometimes seem, (perhaps more than seem) to take on a life of its own.

In his examination of strategies for a catastrophic world Ted G. Lewis explains:

Complex systems evolve discontinuously through space and time... Such systems appear to have no memory; that is the past is not a prelude to the future. Instead the future of a complex system is highly irregular and unpredictable... Systems become more complex as they are improved; as they are made more efficient, less expensive, and more capable. They also become more self-organized. Therefore the more we improve these systems, the more likely they are to collapse unexpectedly.  

This is our reality. A pioneering generation of supply chain innovators has succeeded in a historic transition of their field. A rising generation takes the revolution for granted and can barely imagine the pre-revolutionary reality. The successors are naturally inclined to perceive the progress of the last thirty years as predicting the next thirty years. This is not guaranteed. Given persistent patterns of self-organized criticality found in other complex systems, supply chain problems – even potentially catastrophic problems – are very likely to emerge.

RESILIENCE: READY FOR THE WORST

Before the technological revolution of the last thirty years the supply chain featured much more redundancy, safety inventory, and many more independent players than today. It was less complex, more resilient, more costly, and much less efficient.

Resilience is an innate tendency, usually consisting of several inter-related parts, that allows a system to flex under stress and bounce-back to something similar to its preexisting condition once the stress is lessened or removed.

Complex systems are not inherently less resilient than non-complex systems. But the resilient characteristics of complex systems usually emerge from recurring experience with cascading – occasionally catastrophic – failures. Failure re-opens a complex system to innovation, adaptation, and further optimization. Can we cultivate a resilient supply chain that avoids – or at least mitigates – catastrophic failure?

The contemporary supply chain continues to self-organize and optimize so rapidly that it is difficult to make any certain claims regarding its innate resilience or non-resilience. But there have been examples – most dramatically after the 2011 Japan earthquake-and-tsunami – that suggest the global supply chain behaves in a manner analogous to other complex systems.

Looking at other complex systems, three sources of resilience may be especially promising for the supply chain:

- Diversity (especially in terms of roles and functions);
- Decentralization (and self-organization); and
- Adaptability (even improvisational and opportunistic).
These three characteristics are closely related, especially in terms of the resilient behavior they support. 

Diversity is an effective defense. The functional diversity of a system increases the chance for diversity of response under stress. If even a few individuals or subgroups can effectively adapt to the stress, the entire system is more likely to be preserved and have a chance for recovery. The contemporary supply chain has seen a proliferation of niche players, each with very specific functions that contribute to the supply chain’s overall health. While there are fewer competitors in any particular niche (less structural redundancy) there has been a significant increase in niches (more functional diversity). This functional diversity is a potentially important source of resilience.

Complex systems are innately self-organizing. Feedback mechanisms across a system facilitate the emergence of global patterns from numerous random interactions among widely distributed components. No one controls global effects. The global effects are spawned by spontaneous behaviors that nonetheless produce patterns and rough boundaries that can be predicted. Especially in human-related complex systems, dynamic communications among the participants produce shared behaviors to which the system is attracted and around which system equilibrium unfolds.

Over the last thirty years, as information has begun to drive the supply chain as much as production or transportation, the supply chain has become more and more self-organizing. Randomly distributed demand information determines what patterns will emerge in the global supply chain. While supply capacity has become more concentrated in fewer players and places, the number of demand signals has exploded and the number of distribution players remains highly decentralized.

In 1988 Walmart opened its first grocery-embedded “Supercenter.” There are now over 3,200 Walmart locations offering a full line of food and related products. This has transformed the grocery industry and caused particular stress for traditional supermarkets, such as Kroger, Safeway, and Supervalu. But... the first Whole Foods Market opened in 1980 and in 1988 Whole Foods began sustained expansion at the same time that Walmart was devouring large segments of the grocery market. Whole Foods now has over 300 locations and generates over $9 billion in annual revenue.

In the 1980s the McLane Company grew from a modest regional distributor to a major national provider of food and other products especially to convenience stores and restaurants. In 1990 McLane was purchased by Walmart. But it was not a good strategic fit and in 2003 McLane was sold to Berkshire-Hathaway and reemerged as a largely independent enterprise. It now generates over $34 billion in annual revenue distributing food mostly to non-grocery stores, the most rapidly expanding segment of the grocery industry.

Walmart is certainly the “apex predator” in the ecology of groceries. But its disruptive behavior has opened new niches for other players. Under stress, the decentralized, self-organizing character of the US grocery market has arguably produced greater differentiation and functional diversity. This is a resilient response.

Resilience can mitigate the negative consequences of change through adaptation. Resilience expects change and spawns structural and behavioral characteristics that accept considerable change as a way of avoiding catastrophic change. Diversity does not ensure successful adaptation. A decentralized and self-organizing system produces many mal-adaptive features. But the more diverse and self-organizing the system the more likely the system will generate – nurture and facilitate – effective adaptation.

In the 1970s FedEx emerged from a deregulating transportation sector to challenge many long-time participants in the airfreight business. In just a few years the veterans experienced a catastrophe. But from the perspective of the full eco-system – the US economy and eventually the global economy – FedEx was a positive adaptation to changing conditions. The emergence of FedEx, and other supply chain “species” descended from the FedEx
adaptation, strengthened the US supply chain and national economy especially by increasing diversity and self-organization across the supply chain.

Diversity and self-organization are inputs that increase the likelihood of positive adaptation. Effective adaptation to change – while conserving and strengthening most attributes of the system – is the benefit of resilience. But if adaptation reduces diversity and self-organization the adaptation is non-resilient and moves the system closer to cascading catastrophe.

RELATIONSHIPS: OPTIMIZING DIVERSITY AND SELF-ORGANIZATION

Early in the new century a senior executive with a major supplier to Ford Motor Company told researchers from the University of Michigan and Arizona State University, “In my opinion, [Ford] seems to send its people to ‘hate school’ so that they learn how to hate suppliers. The company is extremely confrontational. After dealing with Ford, I decided not to buy its cars.” 9

In 2010 the North American OEM-Supplier Working Relations survey found:

For the first time in the history of the 10-year-old study that looks at the relationship between automakers and their suppliers, a U.S. automaker – Ford – ranked in the top three. It was third, with Honda and Toyota in 1st and 2nd place, respectively.10

The change in Ford’s behavior has several origins and reflects a broader trend. In the 1980s, when JIT was initially adopted by many US firms, there was much more attention to quantitative outcomes – such as a steep reduction in number of suppliers – than to qualitative inputs, such as the relationships between buyer and supplier. Yet the Japanese practice of JIT emerged from and depended on very dense relationships.

A Japanese Keiretsu – literally “headless combine” – is a grouping of firms that collaborate in design, sourcing, production, and distribution. They are often linked through mutual ownership, joint planning, and a vast web of informal connections. The structural aspects of keiretsu have been long recognized by emulators in the United States, but the cultural dynamics of these relationships were not well understood and tended to be undervalued.

There continues to be substantive qualitative differences. In 2010 twenty-one percent of Ford’s suppliers reported the automaker used threats and retaliation to get price concessions. Only 8 percent of Toyota’s suppliers reported similar behavior.11 The Japanese practice of JIT still gives more emphasis to long-term relationships delivering mutual benefit (voice), while the US practice continues to lean toward survival-of-the-fittest (exit). But there is evidence of adaptation across the supply chain eco-system. In mid-2005 John Paul MacDuffie and Susan Helper argued:

... the “exit” vs. “voice” distinction is no longer as clear as it was just twenty years ago. On the “voice” side, the closed keiretsu system of suppliers characteristic of Japanese industry has been considerably opened to market pressures, requiring more formalization and cost justification of the relationships. On the other, the hard-nosed “exit” approach of U.S. firms has faced pressure for increased collaboration to achieve the increased levels of quality demanded in the market. There has been a wide range of responses to these pressures, often mixed and contradictory. In the U.S. there are frequent attempts to achieve the necessary levels of collaboration without trust; but this approach is marked by internal contradictions which, we believe, make it unlikely that it can stabilize as a lasting model. Thus, we will argue, the industry is converging from all sides on a form of pragmatic collaboration, involving substantial levels of trust, though more open and formalized than the traditional Japanese system.12

This convergence could enhance diversity and self-organization across supply chains. The classic Japanese model nurtured diversity but suppressed self-organization. The US approach to implementing JIT has too often ended up
with carefully controlled — and risk-increasing — sole sources of supply. While far from reflecting mainstream current practice, there is an increasing realization that trusted relationships — both tactical and strategic — are essential aspects of an effective and resilient supply chain. Trusted relationships optimize diversity and self-organization.

To apply for the Malcolm Baldrige Award, sponsored by the National Institute for Standards and Technology, organizations are asked:

What are your key types of suppliers, partners, and collaborators? What role do these suppliers, partners, and collaborators play in the production and delivery of your key products and customer support services? What are your key mechanisms for communicating with suppliers, partners, and collaborators? What role, if any, do these organizations play in implementing innovations in your organization? What are your key supply-chain requirements?

Today it is difficult for many supply chain participants to answer these questions. But there is a growing consensus that these are important practical questions. Being able to honestly respond to these questions with answers that are strategically predisposed to diversity and self-organization makes catastrophic failure less likely.

POLICY RECOMMENDATIONS

On January 23, 2012 the president of the United States released a first-time National Strategy for Global Supply Chain Security. This initiated a yearlong process of private-public consultations. From these discussions a troublesome pattern has been identified: For most of the last generation the private sector search for comparative advantage has resulted in a substantial decrease in the supply chain’s structural diversity. Fewer firms play increasingly important roles.

Until recently this structural concentration in the supply chain was not widely recognized by public policy-makers. But as it has become more apparent — and its vulnerabilities better understood — the inclination by many in the public sector is to increase regulation. Or as more than one official said, “We need to require more redundancy in the supply chain.”

The decline of structural diversity in the supply chain is a potentially significant problem that amplifies every threat by reducing the likelihood of innovative responses to stress. But an increase in traditional modes of regulation will — whatever the effect on diversity — reduce the ability of the system to self-organize, undermining the likelihood of innovation under stress or otherwise. This private-public tug of war threatens to wring out of the system two key components of resilience. This is the kind of optimizing that contributes to eventual catastrophic failure. This is no longer a supply chain that can be yanked one way or another. It is much more a spider-web, even more an ecosystem where what is done in one corner will often have dramatic and unpredictable impacts across the entire system.

Preserving a system’s ability to innovate is fundamental to preserving the system’s overall integrity. Failures will happen. Innovating around failure is how a complex adaptive system continues to emerge. But long-term health is determined by the sort of innovations and adaptations adopted. When diversity and self-organization are maximized, resilience is nurtured. When diversity and self-organization are reduced the next failure is likely to be even worse.

Bureaucracies, both public and private, tend to be suspicious of innovation. There is an inclination to respond to problems with predictable procedures. As procedures accumulate, small failures are suppressed and, in many complex adaptive systems, the likelihood of catastrophic failure is increased. It doesn’t matter if the procedural suppression of innovation is imposed by government regulation or internal management, non-resilience is the outcome.
The Implementation Update for the National Strategy for Global Supply Chain Security (February 2013) signals a continuing coordination role by White House National Security staff and a private-public supply chain working group staffed and hosted by one of the cabinet departments. This could be helpful. It might be a waste of time. Over time it could become dangerous. Much depends on behavior and that is a reflection of who and how and why.

The presumption when private and public meet is – whatever the stated purpose – the eventual agenda relates to rule making and boundary setting by the government. As such, the process is subversive to diversity, self-organization, innovation, and resilience. “Evidence has accumulated that externally imposed rules tend to “crowd out” endogenous cooperative behavior.”13 Stakeholder cooperation in setting norms is especially important in dynamic systems such as the supply chain. In complex adaptive systems rules and boundaries quickly lose influence without active self-monitoring and sanctioning by those involved day-in and day-out, even minute-by-minute, within the system. Some studies have found that externally focused regulation can even “undermine subsequent cooperation” in developing norms.14

Put another way: When dealing with a complex adaptive system rule breaking can be sanctioned after the fact by external rule-makers. But if prevention of rule breaking is the goal the rules must be developed and enforced by system participants.

The global supply chain has become a complex adaptive system. As with most complex adaptive systems – and especially human-influenced systems – it is self-optimizing. If and when optimization reduces diversity and self-organization the possibility of catastrophic failure increases. Most evidence suggests this is the current trend-line for the global supply chain.

Government action focusing on traditional approaches to regulation would accelerate the movement toward catastrophe. But there is another option. Social manifestations of complex adaptive systems can be influenced by intentional social behavior. Precisely because government is not engaged as a competitor or vendor in the supply chain (and is an important customer), the government could serve as a facilitator or honest broker of boundary-setting, rule-making, and system sanctioning by supply chain stakeholders themselves.

The Cross-Sector Supply Chain Working Group called for in the White House Implementation Plan could become neutral ground for ongoing communication among supply chain stakeholders. The National Security staff official(s) assigned to coordinate this process would certainly not be any kind of White House Czar. In most ways s/he would need to be an anti-Czar, a latter-day Metternich composing and facilitating a supply chain world symphony with as much skill as the old Count conducted the Concert of Europe.

This is unlikely. Count Metternich was unique and the complexity of Post-Napoleonic Europe pales in comparison with the modern supply chain. Catastrophe is much more likely and from the collapse of market-leaders, nation-states, and legacy systems something better may emerge. This is the role of catastrophe.

If supply chain catastrophe is to be avoided or mitigated diversity and self-organization must be optimized. This combination – diversity, self-organization, leading to innovation and adaptation – is the strange attractor at the heart of the supply chain’s revolutionary transformation. The deeper the system’s diversity and the more inclusive its self-organization the greater the system’s resilience.

Can the anti-Czar remember this? Can a private-public panel behave consistently with this purpose and direction? Can a complex adaptive system fail and innovate and fail some more, skating along the cusp of catastrophe but always sliding back into the deep basin of diversity, self-organization, and innovation?

Back to Metternich: In his early text, A World Restored, a young Henry Kissinger explains how the Austrian Count and others crafted the Concert of Europe.
...the spirit of policy and that of bureaucracy are diametrically opposed. The essence of policy is its contingency; its success depends on the correctness of an estimate which is in part conjectural. The essence of bureaucracy is its quest for safety; its success is calculability. Profound policy thrives on perpetual creation, on a constant redefinition of goals. Good administration thrives on routine, the definition of relationships which can survive mediocrity. Policy involves an adjustment of risks; administration an avoidance of deviation. Policy justifies itself by the relationship of its measures and its sense of proportion; administration by the rationality of each action in terms of a given goal.¹⁵

If supply chain resilience is to be achieved it must remain a matter of policy rather than administration. Supply chain resilience will not be achieved bureaucratically, but it can be crafted through the intelligent self-conscious give-and-take of authentic private-public collaboration in policy making. Bureaucratic behavior – whether it originates in corporate or government offices – threatens the supply chain. Non-bureaucratic policy makers who persistently nourish diversity, self-organization, and innovation will enable the modern supply chain – and all its benefits – to flourish.

ABOUT THE AUTHOR

Philip J. Palin is the principal author of the Catastrophe Preparation and Prevention series from McGraw-Hill. Other publications include Consequence Management (2008), Threat, Vulnerability, Consequence, Risk (2009), and Supply Chain Resilience: The Strategic Playbook (2012). Mr. Palin chaired the General Preparedness Working Group of the Obama presidential campaign’s Homeland Security Advisory Council. More recently he served as project manager for supply chain resilience in the Mid-Atlantic Regional Catastrophic Preparedness Grant Program. He is a former college president, foundation executive, and corporate chief executive officer. Mr. Palin can be contacted at philipjpalin@gmail.com.

---


10 North American OEM-Supplier Working Relations Study (Planning Perspectives, 2010).

11 Ibid.


In this issue:


Professor Talal Aladwani discusses the concept of the seaworthy container under the Rotterdam Rules.

An update on the Force Majeure Defense is provided by Gregory Buffaloow.

Ryan Hackney considers the interplay between DOHSA and OCSLA in several recent cases involving helicopter death cases in the Gulf.

Michael Marks Cohen explores the benefits and intricacies of the P & I Club Letter of Undertaking.

We provide reviews of several new maritime law books.
The Force Majeure Defense – Recent Cases, Boilerplate and Analysis

Gregory C. Buffalo

I

INTRODUCTION

It is an elementary principle of maritime law that liability must be based on fault. It is therefore arguable that the defenses of force majeure or Act of God are not really defenses, but are instead a shorthand way of arguing that there is no fault where the actual "fault" is that of a vis major or Act of God, or when all reasonable precautions have been taken and yet a [casualty] occurs . . . . " It should be useful, however, to consider typical definitions of these concepts, before analyzing what they really mean, and how the defenses may be lost.

A simple working definition considers the element of control or effects which cannot be anticipated:

FORCE MAJEURE

force majeure (for ma-zh<<schwa>>r). [Law French "a superior force"
An event or effect that can be neither anticipated nor controlled. • The term includes both acts of nature (e.g., floods and hurricanes) and acts of people (e.g., riots, strikes, and wars). — Also termed force majestre, vis major, superior force. Cf. ACT OF GOD; VIS MAJOR.

---

*BA, University of Alabama (Phi Beta Kappa, 1976); JD University of Alabama School of Law (1979); LL.M. (general) New York University (1980). Member, Maritime Law Association of the United States, American, Alabama, and Texas Bar Associations, and Southeastern Admiralty Law Institute. Mr. Buffalo practices in Mobile, AL. Mr. Buffalo is a member of Sutterwhite, Buffalo, Compton & Tyler, LLC, and Chairman of the Marine Section. The writer gratefully acknowledges permission from the Greater New Orleans Bar Federation to publish this paper, an earlier version of which was presented at their 2010 River and Marine Seminar.

1Parks and Cattell, The Law of Tag, Tow and Pilotage, p. 222, 239 (3d Ed. 1994) supports the "well-settled rule that liability must be based upon fault . . . ."

2Parks and Cattell, supra. The Parks treatise treats the concepts of inevitable accident, Act of God or vis major interchangeably with the explanatory note, "[S]tating it another way, it is that which a party charged with an offense could not possibly prevent by the exercise of ordinary care, caution and maritime skill." Id., 239–241.
Blacks Law Dictionary (Westlaw 2004). According to one treatise, it is apparent that "courts have been reluctant to reduce the term 'act of God' to any sort of precise or technical definition," and instead "courts have tended to describe the concept with reference to the particular phenomenon with which they are dealing ... [or] to provide definitions in general descriptive terms ..." The following examples are instructive:

- A freak of nature of sufficient velocity and destructiveness to overcome all reasonable preparations;

- Forces of nature being sufficient to overcome all reasonable preparations;

- An unusual, extraordinary, sudden and unexpected manifestation of the forces of nature which man cannot resist;

- An unusual, extraordinary, sudden, and unexpected manifestation of the forces of nature which cannot be prevented by human care, skill, or foresight;

- Accident involving drifting vessel which could not have been prevented by human skill and precaution and a proper display of nautical skills;

- An extraordinary convulsion of nature or a direct visitation of the elements, against which the aids of science and skill are of no avail, and

- An immediate and exclusive operation of the forces of nature, uncontrolled or uninfluenced by the power of man, which cannot be prevented or escaped by any amount of foresight or prudence or reasonable degree of care or diligence.

As will be shown, with an emphasis on recent cases where possible, the common denominator in force majeure case law involves evaluation of essential evidence that the party claiming the benefit of force majeure undertook precautions and reasonable preparation to avoid the consequences of a foreseeable condition. It is not sufficient to merely contend that the casualty resulted from a severe storm or hurricane.

---

7Id.
9Petition of United States, 300 F. Supp. 358, 366 and n. 2 (E.D. La. 1969)(Hurricane Betsy), citing
11Preifeld v. Hennessy, 353 F. 2d 97 (3 Cir. 1965).
12Pioneer Natural Resources USA Inc. v. Diamond Offshore Co., 638 F. Supp. 665 (E.D. La. 2009),
2009 WL 2022362 at *17 (E.D. La. 2009)(Hurricane Ivan).
II
HURRICANES AND HOW THE DEFENSE MAY BE LOST

The initial consideration of force majeure will be made in the context of losses caused by breakaways and other hurricane-related events. It is emphasized, at the outset, that the defense may be lost based on a showing that preparations were inadequate. For example, in the early DI decision, an Owner was held liable for damage occurring when the its barge broke its lines during a storm and drifted into other vessels, based on a showing that the lines held “during the height of the storm,” and failed later when the Owner failed to keep personnel on board “to care for the lines and renew them if action demanded.” The force majeure defense failed because of the finding “[t]he condition of the lines after the occurrence of the accident indicated they did not break suddenly, but after a period of chafing and wearing.” The Court determined that the wind speed did not preclude the Owner from sending aid or making inspection. The failure to exercise reasonable care was also based on the fact that there was sufficient warning or lead time in which to either remove the barge to a more sheltered location, or provide for personnel on board to tend the lines if required. Conversely, where there was a better showing that lines were periodically checked, and that the mooring was approved by a veteran of four hurricanes, the force majeure defense was sustained for damages caused by vessels which broke their lines during severe weather.

III
HISTORICAL DATA AND INDUSTRY STANDARDS

The defense of force majeure is also evaluated based on an analysis of historical data, which should be supported by expert testimony. A good illustration is found in Pioneer Natural Resources USA Inc v. Diamond Offshore Co. In the Pioneer decision, Owners of a underwater pipeline system

---

17The *DI*, 30 F. 2d 250, 251 (2 Cir. 1929).
18Id.
19Id.
20Id. The court focused in a period of 3 1/2 hours in which there was time to inspect and add lines, but nothing was done.
21Id.
22United States v. SS *JOSEPH LYKES*, 300 F. Supp. 358 (E.D. La. 1969)(Hurricane Betsy). The decision also denied a salvage claim by Central Gulf Steamship based on the fact that its moored vessel GREENPORT “was unavoidably struck by the JOSEPH LYKES, whose progress upriver was thereby momentarily checked . . . .” Id., at 366.
23Pioneer, supra, n. 9.
sought recovery of damages against Owners of a drilling rig which became adrift during Hurricane Ivan. The Court ruled in favor of the Rig Owners finding that adequate precautions were taken based design factors for moorings which took into account a ten year history of reported storm conditions.

In the *Pioneer* decision, the facts involved movements of the drill rig OCEAN AMERICA during Hurricane Ivan. During the hurricane, the OCEAN AMERICA broke its moorings and drifted over 18 miles. The *Pioneer* Court concluded there was sufficient evidence of a trench, and found that the Rig had, in fact, damaged Pioneer’s underwater pipelines. The decision in favor of the Owners of the OCEAN AMERICA was based on expert testimony that the Rig was properly secured in advance of the storm and that adequate preparations and a contingency plan had been followed.

The Court credited evidence that applicable industry standards for Mobile Offshore Drilling Units (MODU) were followed for design of the rig moorings, and ruled in favor of the Rig Owners based, in part, on a related finding that the OCEAN AMERICA moorings were designed to withstand ten year storm conditions. The MODU standards required only that the moorings be designed to withstand five year storm conditions. The Court rejected the Plaintiff’s contention that the Rig should have been relocated in advance of the storm, crediting expert testimony that “the idea of a hurricane evasion tow of the OA . . . to be a dangerous maneuver.” The *Pioneer* decision also provides a good inventory of the types of expert testimony which may be required to successfully defend a case of this nature.

The decision in *Pioneer* in favor of the Rig Owners was based on testimony of the expert who drafted the American Petroleum Institute standards applicable to inspection of mooring components, testimony from Plaintiff’s metallurgical engineer who was of the opinion that the Rig anchor chain flattened certain areas of the pipeline, and testimony from a Master Mariner concerning the Tropical Contingency Plan. The Master Mariner

---

9It should be noted that the Defendants contended there was insufficient evidence of a trench cut by the OCEAN AMERICA mooring lines, id. at *41, and argued that there were at least five other offshore drilling rigs that lost station during passage of Hurricane Ivan. Id.
10Id., 2009 WL 2022362 at *8. The Court credited testimony from the expert who drafted the American Petroleum Institute standards applicable to inspection of mooring components, id. at *8.
11Id. at *8.
12The Court credited the testimony from a Master Mariner that a hurricane evasion tow would run the risk of “having rig personnel and attending vessels caught or trapped by the approaching storm.” Id. at *6.
13The listing of experts and brief summary of testimony included offshore engineering experts, mechanical engineers, naval architects, metallurgical engineers, experts in testing metallurgy materials, oceanographers, experts in mooring design as well as Master Mariners.
14Id. at *8
15Id. at *3
16Id. at *4.
provided the basis for the finding that there was “no negligence in . . . [executing] the planned relocation of the rig OA less than two miles away . . . instead of attempting a hurricane evasion tow . . . as suggested by plaintiffs.”

IV
PRECAUTIONS BY OTHER VESSELS IN PROXIMITY

It was also significant that at least five offshore drilling rigs lost station during the hurricane. The Pioneer Court made specific reference to the fact that “five semi-submersibles rigs parted their moorings” in the conclusion of law that “Hurricane Ivan was a classic ‘Act of God.’” Had the preparations been adequate for some of the rigs in the relevant area, it is believed the outcome would be different, because the fact that other rigs in the area remained secured, and without drifting, would be an indication that it was indeed possible to design a mooring system based on the facts known at the time of the preparations. For example, in a decision involving adequacy of preparations for Hurricane Katrina, In re Atlantic Marine, summary judgment was denied the Owner of a Barge that broke loose during the hurricane based on the fact “that other rigs in the same area, and in areas closer to the eye wall of the hurricane, were submerged and did not break loose.” Trial was required in Atlantic Marine based on the simple analysis that “[t]he only clear fact is that the preparations actually made were insufficient since the moorings failed.”

V
FORECASTING ERRATIC HURRICANE PATH

The Pioneer decision should not be read as a general endorsement of failure to consider hurricane evacuation. While the Pioneer Court found evacuation was not feasible under the facts presented, it should be remembered that the erratic and unpredictable route for Hurricane Ivan was a factor in which the Court did not find fault with the Defendant’s decision to move the rig only two miles. The Pioneer Court noted that the forecast for the storm

---

2Id. at #7.
3Id. at #18.
5In re Atlantic Marine, supra, 570 F. Supp. at 1376. There was also expert testimony that “if the [rig] had been moored correctly that it would have been able to withstand winds of 70 – 75 and even 120 mph.” Id., at 1376 – 1377.
6Id., at 1377.
trended initially to the East Coast of Florida prior to September 6th, the forecast was later pulling toward the West on September 6th, then shifted back to the East at 5:00 a.m. on September 7th; and finally turned back towards Florida by 11:00 p.m. on September 7th. The finding that evacuation was not required was based on the conclusion “[s]uffice it to say, there was an 85% chance that the Ocean America would be on the east side — i.e., the good side of the storm. As late as 5:00 p.m. on September 11, 2004 the forecast was landfall on the Florida panhandle.” Other factors relevant to feasibility of removal or evacuation include the amount of time in which to react, and existence of obstructions in the area.

With assistance of qualified expert witnesses, it should be possible to make similar arguments that the likely storm track of any hurricane is extremely difficult to forecast.

Despite aircraft, land, and shipboard reconnaissance, weather satellites, and other sources of data, the exact path a hurricane will take is rarely predicted with precision. Instead hurricane tracks exhibit “humps, loops, staggering motions, abrupt course and/or speed changes, and so forth.” Indeed, no two, recorded, severe tropical cyclone tracks have ever been exactly the same in any ocean.

VI

CONTINGENCY PLANNING

The approach of a hurricane or other severe weather conditions necessarily involves a consideration whether there is sufficient time to better secure the affected vessel or ample time for evacuation. Contingency planning should therefore involve attempts to locate alternative facilities well in advance, and identify potential weather experts who may be required in litigation.

---

1Id., at 66.
2Id.
3See, United States v. Barge CBC 603, 233 F. Supp. 85 (E.D. La. 1964). In Barge CBC, the Barge owner had several hours notice that the water level would be raised in the area of the barge due to waters released by a dam, but the Owner was not faulted for failure to remove the barge. The Court found “a removal of the barge was not feasible . . . due to an obstruction . . .” Id., at 89.
5In Atkins v. Alabama Drydock & Shipbuilding Co., 195 F. Supp. 944, 947 (S.D. Ala. 1960) (Thomas, J.) the owners of a drill rig were held liable for damage resulting from a breakaway during a storm based on a conclusion “there was ample time to better secure the rig for the anticipated conditions” based on the findings that the damage occurred between ten-thirty and eleven in the evening, and the forecast was given at 3:30 p.m. for 35 mph winds with gusts up to 52 1/2 mph.
Difficulties are likely in locating alternative locations for a safe harbor, on short notice, and particularly abroad. Operators of oceangoing tugs, for example, should be mindful of the situations involving the ERIKA and the CASTOR.\(^3\) In December of 1999 in the face of winds up to sixty miles per hour, the tanker ERIKA although citing structural problems, was refused access to the French Port of Saint Nazaire.\(^4\) The French authorities initially denied a request call was made, and later requested assistance from the British Royal Navy.\(^5\) Similarly, in December of 2000, the tanker CASTOR encountering a Force 12 gale was denied access to Monaco, Algeria, France, Gibraltar, Greece, Italy, Malta, Spain and Tunisia.\(^6\) While considerations of a vessel's right of entry\(^7\) versus the port or coastal states' right of self defense\(^8\) are beyond the scope of this paper, it is suggested that as a matter of good risk management and contingency planning, the careful operator will make advance preparation to identify alternative places of refuge.

VII

EVACUATION OR HURRICANE CLAUSES

A related consideration is whether the marina or fleeting area may require vessels to evacuate. The wharfinger may provide notice to evacuate to avoid potential exposure. An illustration of wharfinger's liability is provided in Compania de Navigacion Porto Ronco v. SS AMERICAN ORIOLE\(^9\) in which the Defendant shipyard was held liable for damages resulting when a vessel broke away from its berth during forecast bad weather, and drifted downstream. The decision was based on a wharfinger's duty to exercise reasonable care to adequately secure a vessel in the face of impending bad weather.\(^10\) The force majeure defense was rejected based on evidence it was possible to better secure the vessel because the nearby SS GALAXIAS,

\(^{1}\)Murray, "Any Port in a Storm? The Right of Entry for reasons of Force Majeure or Distress in the wake of the Erika and the Castor," 63 Ohio St. L. J. 1465 (2002).

\(^{2}\)Id., at 1470.

\(^{3}\)Id.

\(^{4}\)Id., at 1471.

\(^{5}\)"When a ship is forced to transit through the territorial sea of a state and stop there, for reasons of force majeure or distress, such passage is deemed innocent. This principle, incorporated in UNCLOS, is an ancient and well-established principle of customary international law." Murray, supra, 63 Ohio St. L. J. at 1474-1475.

\(^{6}\)"Coastal states have an inherent right of self-defense. This right in some circumstances arguably gives states the right to keep dangerous ships away from their shores . . . [and] to protect their populations and their environmentally sensitive coastal areas." Id., at 1467.

\(^{7}\)474 F. Supp. 22 (E.D. La. 1976), aff'd, 585 F. 2d 1326 (5 Cir. 1978).

\(^{8}\)Id., 474 F. Supp. at 27.
approximately 200 feet away, did not break away from her moorings. The vessel was unmanned and there was no consideration of fault of the Owner.

In the situation where the wharfinger seeks to require evacuation, the notice is likely to be based on tariff or contract provision requiring removal in the event of a hurricane warning. A similar provision of a dock license that "requires removal of all vessels from the marina at the time of or before the issuance of hurricane warnings for the area" was considered in *Northern Insurance Co. of New York v. Pelican Point Harbor, Inc.* In *Northern Insurance*, owners of the Yacht *Charmer* were requested by the Harbor Walk Marina to remove their seventy foot craft due to issuance of a hurricane watch for Hurricane Ivan which was approaching Destin, Florida. The yacht was then anchored in Destin Harbor to ride out the hurricane.

After the storm the yacht was found severely damaged in Chocktawhatchee Bay. The subrogated insurance carrier paid $655,000 to the Owners for a constructive total loss and then sought recovery as subrogated Plaintiff from the marina. The subrogated carrier, Northern Insurance, made claim based on alleged breach of contract and negligence *per se*. The negligence *per se* argument was based on a Florida Statute which prohibited forced evacuation of vessels from marinas following issuance of a hurricane watch or hurricane warning. The Court entered summary judgment dismissing the negligence *per se* claim based on an analysis of Florida law that the statute did not create a private cause of action or civil remedy for alleged violation of the Act, because it provided for criminal penalties. The *Northern Insurance* decision nevertheless found admiralty jurisdiction for a breach of contract claim "based on defendants' demand that [the Owner] remove the *Charmer* from its boat slip as Hurricane Ivan approached, which resulted in the constructive total loss of the vessel . . . ." Admiralty jurisdiction was based on an analysis of whether the Defendant's conduct, which occurred on land, was a tortious act because "for purposes of the jurisdic-

---

4Id.

42006 AMC 1586, 2006 WL 1285078 (N.D. Fla. 2006).

4The Florida Vessel Safety Law, Fla. Stat. §327.59(1) involved in the opinion, provided, in part, as follows:

After June 1, 1994, marinas may not adopt, maintain, or enforce policies pertaining to evacuation of vessels which require vessels to be removed from marinas following the issuance of a hurricane watch or warning, in order to ensure that protecting the lives and safety of vessel owners is placed before interests of protecting property.

4Id., 2006 AMC at 1597. The Act provided that violation constituted a misdemeanor punishable by up to 30 days in jail, Fla. Stat. 327.72 or by payment of fine for initial offense up to $250, Fla. Stat. §327.73.

4Id., 2006 AMC at 1588.
tional locality test the tort occurred on navigable waters." The *Northern Insurance* decision also suggested additional mediation of the remaining maritime law count, and noted that triable issues included whether there was ample time to motor or trailer the vessel to a safer location, whether equipment used to secure the *Charmer* in Destin Harbor was adequate, whether the Owners were inexperienced at securing the *Charmer* to ride out the storm, and whether expert testimony supported a claim the vessel would likely have survived the storm with minimal damage had she remained in her slip at the marina. The foregoing is simply a re-statement of the usual issues in a force majeure analysis of whether precautions were adequate, sufficient time existed to act, and whether the parties exercised reasonable care.

A Florida State Court decision, *Burlow & Assoc. Inc. v. Belcher*, involving the same statute, dismissed a marina owner’s claim for damage to the facility resulting from alleged failure to abide an evacuation notice. The *Burlow* decision concluded that general maritime law did not preempt the Florida statute, “because the statute does not threaten the uniformity of federal maritime law, which does not specifically address the issue of evacuation of marinas in the face of a hurricane threat.” This conclusion was based in part on a brief survey of maritime cases with arguably differing results on the factual inquiry whether relocation was required. In the *Burlow* decision, the Court reviewed *United States v. Bruce Dry Dock*, which imposed liability on a vessel which refused to comply with a request two days prior to a hurricane to relocate, that subsequently broke moorings during a hurricane and destroyed a floating drydock. The basis of the *Bruce Dry Dock* decision was expert testimony that the offending vessel “would have been in a safer position if she had been anchored in the bay.” The Court compared this result with *The Havana*, *Tvety v. Houseboat Jilly*’s

---

"See discussion of *Executive Jet*, and finding that "[t]he alleged act of requiring removal of a boat from a marina immediately prior to landfall of a hurricane certainly has the potential to disrupt maritime commerce . . . ." *Id.*, 2006 AMC at 1591–1592.

""[A]lthough the parties have previously mediated this case without success, the court believes additional mediation of Count One, plaintiff’s breach of contract claim, should be conducted." *Id.*, 2006 AMC at 1598.

*Id.*, at 1594.

*Id.

*Id.

*Id.*, at 1595.


*Id.*, at 719 So.2d 35.

*65 F.2d 938 (5 Cir. 1933).

*Id.*, at 38.

*89 F.2d 23 (2 Cir. 1937).*
Yen,

and Ladner v. Bender Welding and Machine Co.,

in which suits for damages were dismissed against vessels which broke moorings during severe weather, based on findings that the vessels had been properly moored.

The Burlow decision also suggested, in dictum, that evacuation clauses may be void:

We leave for another time, because it was not presented in this case, the question of whether so-called “hurricane clauses” in slip lease agreements (requiring the boat owner to remove the vessel from the marina upon threat of hurricane) would be void as against this public policy, even in the absence of section 327.59.

A recent law review article suggests, for example, such evacuation clauses may be void as against public policy “by requiring the owner, despite having paid a docking fee, to embark on a dangerous journey in what could be considered a futile attempt to seek safe haven.” There are also obvious difficulties with proof in such cases whether, or to what extent, damages were caused by vessels which were not evacuated from the facility as opposed to vessels which “were carried by wind and tide” into the facility.

Some guidance on the evacuation issue is provided in recent Hurricane Katrina cases in which Mississippi Federal Courts have dismissed claims filed by property owners for damages caused by shipping containers and cargo which had remained in the Port of Gulfport prior to the hurricane. In Royal Beach Hotel v. Crowley Liner Services, and Defazio v. Chiquita Fresh North America LLC, similar claims were dismissed. In the Royal Beach Hotel decision, while the Court recognized Crowley owed a duty to take reasonable precautions, it found that appropriate precautions were taken, and determined as a matter of law that, because of the unprecedented nature of Hurricane Katrina, there was no duty to take additional measures.

Certainly Crowley owed a duty to plaintiffs, as the owners of real property in close proximity to its port operations, to take reasonable measures to prevent containers, trailers, chassis, and other items under Crowley’s control, from washing away in the event of a storm. However, the court holds as a matter of law that Crowley did not breach this duty because it did, as a matter of uncontested fact, take all measures as were prudent and reasonable under the cir-

---

Bal lett, supra, 719 So. 2d at 36 n.4.
Id. “Apportioning the liability will prove difficult in light of the magnitude of the post-[hurricane] wreckage.”
2007 WL 1499815 (S.D. Miss. 2007).
2006 WL 2788732 (S.D. Miss. 2006).
circumstances in the short period of time between the issuance of the warning and the actual arrival of the hurricane. The court also holds, as a matter of law, that defendant had no duty to take additional measures, beyond those described below, because the enormously destructive force of Katrina was unprecedented and defendant could not reasonably have foreseen that its containers, trailers and chassis might wash and blow away and cause damage to neighboring property unless additional, extraordinary measures were taken to secure them.\textsuperscript{39}

The \textit{Royal Beach Hotel} decision is interesting because summary judgment was entered notwithstanding the fact that there were admittedly some factual disputes.\textsuperscript{40} Both cases involved an analysis of the block stowage which had been used, supported by expert testimony, and the fact that block stowage "is often incorporated into hurricane contingency plans."\textsuperscript{41}

\textbf{VIII}

\textbf{CONTRACTUAL FORCE MAJEURE PROVISIONS}

While the initial focus of this paper has been on application of force majeure in the context of avoiding exposure for breakaways during hurricanes and severe weather, force majeure clauses are also frequently involved in towing contracts. Typical force majeure provisions in a towing contract may seek to absolve the parties from damages for cargo loss, or from damage which occurs to its tow. A good illustration of clauses related to claims for cargo loss is provided in \textit{Enron Petrochemicals Co. v. Barge DXE 233},\textsuperscript{42} which involved a claim for damages against Dixie Carriers for alleged contamination of a shipment of ethanol carried in a Barge owned by the Defendant.

\textbf{IX}

\textbf{CARGO LOSS}

Two principal exculpatory clauses of the governing Charter were in issue in the \textit{Enron} decision. The Defendant relied on a Clause entitled Insurance and Marine Perils, and the Plaintiff relied on a similar clause entitled force majeure, which it contended required exercise of due diligence. Excerpts from each of the clauses are quoted.

\begin{itemize}
  \item \textsuperscript{39} \textit{Royal Beach Hotel}, supra, 2007 WL 1499815 at *2.
  \item \textsuperscript{40} The mere existence of some alleged factual dispute between the parties will not defeat an otherwise properly supported motion for summary judgment. \textendash{} Id., at *1.
  \item \textsuperscript{41} \textit{Defazio}, supra, 2008 WL 2788732 at *5, \textit{Royal Beach Hotel}, supra, 2007 WL 1499815 at *4.
  \item \textsuperscript{42} 98 F. 3d 1338, 1996 WL 556855 (5 Cir. 1996).
\end{itemize}
The District Court concluded that Clause 22 precluded Enron from recovering from Dixie Carriers\(^2\) and the Fifth Circuit affirmed.\(^7\) This Clause provided as follows:

**INSURANCE AND MARINE PERILS:** . . . [Enron] hereby acknowledges that the towage rate specified herein does not contemplate or include liability for loss of or damage to the cargo or an allowance for liability insurance covering the cargo, and as additional consideration supporting [Dixie's] undertakings[,] ... shall and it does hereby agree to hold [Dixie] ... harmless from claims for cargo . . . contamination, whether arising or resulting from an act of neglect or default in the navigation or management of the tow, including but not limited to explosion, fire, collision, stranding, salvage, operations, equipment defects, or other peril, danger or accident of navigable waters or from any other cause of whatsoever kind arising. In furtherance hereof, [Enron] agrees to secure and maintain in effect a contract of cargo insurance, to the full market value of all cargoes transported hereunder, insuring against all marine risks and perils, including loss, damage, contamination, salvage and general average contributions, etc., and to have [Dixie's] name inserted as an additional insured in said policies, with loss payable to [Enron] and [Dixie] as their respective interests may appear, and [Dixie] shall be deemed to be co-insured, whether so named or not, or to secure a waiver of assignment and/or subrogation from the cargo underwriters in favor of [Dixie] on account of any cargo claims paid by such underwriters. In the event that [Enron] shall fail to procure and maintain insurance as provided herein, [Enron] shall be liable to and hold [Dixie] harmless from any claims or demands, losses, cost and expenses, to the same extent that the required insurance would have protected [Dixie]: and in any claim or suit for cargo loss or damage, it will be presumed that such insurance, if it had been procured and maintained would have covered the occurrence, loss or damage in question . . . .\(^7\)

The Court also considered the Plaintiff's arguments based on a force majeure clause which provided as follows:

**FORCE MAJEURE:** [Dixie] . . . shall not, unless otherwise in this charter expressly provided, be responsible or liable in any way for any loss or damage or for any failure or delay in performance hereunder, arising or resulting from: . . . unseaworthiness of the tow unless caused by want of due diligence on the part of [Dixie] to make the tow seaworthy or to have it properly manned, equipped and supplied: or from any other cause of whatsoever kind arising without the actual fault or privity of [Dixie].\(^7\)

The Enron Court rejected an argument that Clause 22 was a waiver of liability, finding it was merely a compulsory insurance clause that properly shifts the cost of procuring cargo insurance from the carrier to the shipper.\(^26\)

---

\(^1\) *Enron*, supra, at *1.
\(^2\) *Enron*, supra, at *4.
\(^3\) *Enron*, supra, at n. 1.
\(^4\) *Enron*, supra, at n. 2.
The basis of the holding was an earlier case, *Twenty Grand Offshore Inc. v. West India Carriers, Inc.*, which found that another insurance arrangement requiring a Tug and Tow to each insure their respective vessels, requiring a waiver of subrogation and a designation of the other party as an additional insured, were not invalid or unenforceable as exculpatory clauses contrary to *Bisso v. Inland Waterways Corp.*, which had prohibited a contractual exemption of a towboat owner from responsibility for his own negligence. The justification was that “in return for a lower shipping charge, Enron agreed to pay for the cargo insurance that Dixie normally would provide.”

The *Enron* Court also rejected the contention that the force majeure clause should impose liability based on breach of a warranty to use due diligence finding that Dixie “is still liable for any damage that the cargo insurance normally does not cover.” A similar clause releasing the Barge owner from any exposure for cargo loss was rejected in *Hartford Accident & Indemnity Co. v. Gulf Refining Co.*. The action involved explosion of a gasoline barge being unloaded at a refinery. The Barge Line sought to avoid liability for the loss of cargo destroyed in the explosion and fire. The *Hartford* Court rejected the argument that the Towing Company was not responsible for loss of cargo despite a clause providing the cargo was transported at the “sole risk of such cargo.” The “sole risk” language was modified by subsequent provision in the same clause which required “reasonable care ... in the receipt, stowage, handling, care and delivery of the cargo ... until the products reach the shore line hose connection in unloading.” The *Hartford* Court also rejected application of a force majeure clause, asserted as an alternative defense, which also required a showing that the cause was beyond control of the Charterer, tow, or Owners. The force majeure clause in issue is quoted as follows:

*Force Majeure*: Neither Owner, Charterer, the tow, her master or owners, nor any other equipment used by Owner, shall be responsible or liable or in any way for any loss or damage, or for any failure or delay in performance hereunder arising or resulting from: Acts of God. Perils of the waters, or of navigation, strikes or stoppage of labor for whatever cause, fire, explosion, neglect, default or barratry of the master or crew, enemies, pirates, assailing

---


3 Id., at 7, discussing "the proper way for Enron to challenge Dixie's claim that it is free of liability is to argue that standard cargo insurance does not cover breaches of the duty to use due diligence. Enron, however, conceded ... that if the argument is given effect, Dixie is absolved from liability."

320 F.2d 346 (3 Cir. 1956).

3 Id., 320 F.2d at 355 n. 9.

3 Id., at n. 9.
thieves, seizures, arrest or restraint of princes, rulers or people riots or civil commotion, compliance with any law, rule, order, regulation, restriction, recommendation or request of any government or agency thereof or any person purporting to act under authority thereof or any other cause, whether similar or dissimilar to the foregoing, which is beyond their control." 

The trial court rejected both clauses based on a factual determination that "Black Warrior's employees were negligent in commencing the discharge operation without the blind flange on the outboard end of the line" which contributed to cause of the explosion.

X
DETECTION BY CUSTOMS

Force majeure clauses which are applicable by contract occur in other contexts as well. For example, in *Domar Ocean Transport Ltd. v. Independent Refining Co.*" such a clause in a contract to provide a tug and tank barge for transport of slops from an oceangoing vessel, disclaiming liability of either party in the event of "arrest or restraint of princes, rulers or people," was given effect to limit liability for payment of hire during a period between January 5 to March 18 in which the barge was under Coast Guard seizure because of improper Customs declarations.

The result in *Domar* would appear to be inconsistent with the general rule, however, that the restraint of princes exception should not apply where the beneficiary of it was partially responsible for the seizure. "Just as a party deliberately exposing himself to the operation of a 'restraint of princes' is deprived of the right to rely on the exception, similarly, where a party's carelessness has brought about the operation of a 'restraint of princes, he is not able to rely upon the exception."

XI
CONTRIBUTING FAULT

Fault of the party claiming the benefit of a contractual force majeure clause, which contributes to the incident, may bar application of the exception. In *Saigon Flour Mills v. General Supply Agency,* the shipper sought

"Id., at n. 10.
"Id., 230 F.2d at 350.
"783 F.2d 1185 (5 Cir. 1986).
"Id.
"Cooke, *Voyage Charters,* ¶85.300 "Arrest or restraint of princes, rulers or people, or seizure under legal process," at p. 976 (2d Ed. 2001).
The Force Majeure Defense

return of prepaid freight following a stranding. The carrier relied on a force majeure clause providing it could retain 90% of the freight if "the vessel is lost or unable to proceed to destination after completion of loading as a result of . . . stranding without the fault of the carrier; jettison; fire from any cause; Act of God . . . " Repayment was required and the force majeure defense was rejected based on the conclusion that faulty navigation was the cause of failure to deliver the cargo instead of the asserted tropical storm and Force 7 – 8 winds. Similarly, while strikes may be excluded in a force majeure clause, application of the defense may be rejected where there is a showing that the party invoking the strike provision assumed the risk. A carrier may contractually exclude hijacking provided its agents or servants were not an accomplice.

XII

DETENTION BY THE COAST GUARD

In Aron & Co. v. Cargill Marine Terminal, government action provided a force majeure defense to a claim for total loss of grain cargo where four barge loads of grain were subject to deterioration due to delays in transit on the Mississippi River for several weeks when the U.S. Coast Guard closed the river to navigation due to extensive flooding in the Midwest. Normally the transport would have taken about 20 days but the closing delayed discharge of the barges from 70 to 121 days depending on the time of loading. The Court therefore determined "the grain deteriorated as a result of natural processes of temperature and moisture in the cargo . . . [and] the moisture conditions were not caused by any water penetration of the barge." Successful application of the clause based on unanticipated flooding and government action, again involved an analysis whether there was contributing fault of the carrier. The force majeure clauses from the governing Contract of Affreightment successfully invoked in Cargill Marine are quoted as follows:

15. CARGO LIABILITY: Liability is assumed for general average, salvage charges and physical damage to or loss of the shipment howsoever occurring (including but not limited to fire, explosion, marine perils and Acts of God);

Id., at 1500.

Id., at 1503.

In re Ninha Offshore Corp., 1973 AMC 1060 (Arb. at NY 1973) (Charette aware of strikes against the flag of the vessel at destination when it scheduled the voyage).


Id., at 2289.
provided that the carrier shall not be liable for delay in the delivery of the shipment, or for loss of, damage to, or any expense in connection therewith, caused directly or indirectly by or resulting from or arising out of; shrinkage, expansion, or other change due to natural causes; any vice or defect in the shipment; the act or default of the Shipper or owner; insufficiency of packing; improper stowage, or the physical act of loading or unloading, when not performed by Carrier; the authority of law; including without limitation, quarantine and embargo; or the acts of the public enemy, hostilities or warlike operations; whether or not there be a declaration of war.

17. FORCE MAJEURE: Except as provided in Article 8 hereof, neither party shall be liable for any loss or damage or from failure to perform or for delays in performance resulting from and occasioned by . . . Acts of God or the elements, river or lock outages, perils or accidents of the sea or other water, . . . or any other cause whatsoever beyond the control of the respective parties, whether the kind enumerated or otherwise.  

Detention by the Coast Guard was rejected as a basis to declare force majeure in Philips Puerto Rico Core Inc. v. Tradex Petroleum Ltd., 67 where the carrier made prompt arrangements for mitigation, and substitution of a carrying vessel. The detention by the Coast Guard was based on concern whether the OXY TRADER, an integrated tug and barge, was safe for deepsea transport, based on a contemporaneous report of the sinking of a similar integrated tug and barge the OXY PRODUCER. 68 There was reported concern that both vessels had a similar design defect. The Coast Guard detention occurred on September 25th and by October 7th the Carrier indicated it would arrange for transshipment. 69 The Shipper provided notice of Force Majeure and reserved the right to cancel the contract. 70 Actual transshipment began on November 13th. 71 The force majeure clause in issue is quoted in full:

FORCE MAJEURE: In the event of any strike, fire or other event falling with [in] the term ‘Force Majeure’ preventing or delaying shipment or delivery of the goods by the seller or occurrence prior to shipment or delivery and preventing or delaying reception of the goods by the buyer, then the contract period of shipment or delivery shall be extended by 30 days on telex request made within seven days of its occurrence. Should shipment or delivery of the goods continue to be prevented beyond 30 days, the unaffected party may cancel the unfulfilled balance of the contract. Should the contract thus be can-

---

67 Id., at 2288.
68 782 F. 2d 314 (2 Cir. 1985).
69 Id., at 316.
69, 71 Id., at 316–317.
70 Id., at 318.
71 Id., at 317.
The Force Majeure Defense

XIII

BURDEN OF PROOF

The Tradax court determined that force majeure was inapplicable, and ruled against the Shipper, finding that the notice of force majeure and attempts to terminate the contract constituted premature repudiation which amounted to breach of contract. The ruling in favor of the carrier was based on the immediate efforts by the provider of the integrated tug and barge to mitigate, and the Court concluded that the Shipper, as the party asserting force majeure, had failed its burden of proof. The holding provides a good summary of the general rules of construction and burden of proof:

We also look to the basic purpose of force majeure clauses, which is in general to relieve a party from its contractual duties when its performance has been prevented by a force beyond its control or when the purpose of the contract has been frustrated. See, e.g., Nissho-Iwai Co., Ltd. v. Occidental Crude Sales, Inc., 729 F.2d 1530, 1540-42 (5th Cir.1984); Gulf Oil Corp. v. FERC, 706 F.2d 444, 452 (3d Cir.1983), cert. denied, 464 U.S. 1038, 104 S. Ct. 698, 79 L.Ed.2d 164 (1984). See generally 3A A. Corbin, Corbin on Contracts, § 642 (1960); Squillacote & Congleton, Force Majeure, 80 Comm. L.J. 4 (1975).

The burden of demonstrating force majeure is on the party seeking to have its performance excused. 3A A. Corbin, supra, § 642 at 73 & n. 41, and, as Judge Carter pointed out, the non-performing party must demonstrate its efforts to perform its contractual duties despite the occurrence of the event that it claims constituted force majeure. See, e.g., Gulf Oil Corp. v. FERC, supra, 706 F.2d at 452.

The result is consistent with the suggested analysis of hurricane and severe weather force majeure situations in which the Courts appear to be guided by evaluation of the reasonableness of the actions taken. In an extreme situation in which claims of force majeure are baseless or without merit, there is authority supporting an award of punitive damages for fraud against the party asserting force majeure notices “without a legal, factual basis.”

---

"Id., at 320.

"Id.

"Id., at 319.

XIV
OTHER GOVERNMENTAL ACTION

Additional illustrations of contractual force majeure clauses involve excuse of delay in payment due to government "red tape" in currency transfers,\(^\text{10}\) cancellation of a voyage based on a contract term specifying "delay on the Railway or in the Dock,"\(^\text{11}\) and attempted excuse of demurrage based on delays in transiting the Panama Canal attributable to Canal Zone employees based on a force majeure provision that "excludes any liability for delay resulting from . . . public or proprietary acts of any governmental authority."\(^\text{12}\)

A more restrictive view of "government action" would limit the term to acts by the specific governmental body with authority to act.\(^\text{13}\) Government

\(^{10}\)In re Cochin Refineries Ltd., 1978 AMC 444, 448 (Arb. at NY 1978)(late payments due to Indian Government currency exchange rules excused under force majeure exception). The force majeure clause relied on was as follows:

Charterer shall not be liable for demurrage, loss, damage, claims or demands of any nature whatsoever incurred or suffered by Triton, Owner of the vessel, due to delays or defaults in performance under this contract caused by acts of God or the public enemy; perils of navigation; floods; fires; hostilities; war (declared or undeclared); executive or administrative orders or acts of either general or particular application of any de jure or de facto government or of any person purporting to act under the authority of any such government, or requests of any such person purporting so to act; illegality arising from applicable domestic or foreign laws or regulations; blockade; labor disturbances; strikes; riots; insurrections; civil commotion; quarantine restrictions; epidemics; floods; storms; earthquakes; accidents, explosions; breakdown or injury to, or expropriation, confiscation or requisitioning of, raw materials or producing, manufacturing, selling, delivery or receiving companies or facilities; abnormal decline or exhaustion of crude oil production; any change in the characteristics of oil available for delivery at loading port which would not permit Charterer's supplier to deliver oil; partial or total interruption, loss or shortage of transportation facilities; failure of carriers to transport or furnish transportation facilities; imposition of restrictions or onerous regulations by any government or governmental agency, or by rationing or allocation, whether imposed by law or assumed as the result of the voluntary cooperation of industry at the insistence or request of any government or of a person or authority purporting to act for any government; reduction or cessation of production of oil by reason of imposition or threatened imposition by any government or person purporting to act with governmental authority of conditions or requirements which in the reasonable judgment of Charterer's supplier make it necessary to cease or reduce production of oil; by the election of the government to take royalty oil in kind; or by any event which shall not reasonably be within the control of Charterer, whether similar to the causes specified above or not. The foregoing causes or events excusing delays or defaults in performance by Charterer when they affect Charterer shall also excuse delays or defaults in performance by Charterer when they affect Charterer's supplier.

\(^{11}\)In re Hermes Shipping, 1970 AMC 2203 (Arb. at NY 1970).

\(^{12}\)Foss Maritime Co. v. Cushman Equipment Co., 2008 WL 4534378 at *4 – 5 (E.D. La. 2008)(question of fact presented whether Canal Zone employees or Cushman were responsible for delays in transiting Canal).

action covered by force majeure also includes confiscation of cargo. A final illustration of government action which permitted termination of carriage of a grain cargo based on force majeure involved the United States termination of government financing of grain shipments to East Pakistan for wheat contracted but not yet shipped. Cancellation was allowed even though the United States had not banned shipments to Pakistan.

XV
TERRORISM AND PIRACY

Force majeure clauses also typically exclude losses due to acts of piracy. For example, the clause referenced in the Hartford decision made specific reference to “pirates.” Specificity of language is essential, however, as the legal definition of terrorism may not be as broad as might be expected. For example, in Miller Marine Services, Inc. v. Travelers Insurance Co., sinking of a vessel attributed to intentional acts by disgruntled former employees was not considered terrorism.

As a precaution, it is suggested that agreements containing more general language, such as the force majeure clause in the Bimco standard barge charter form, should be supplemented to make specific reference to piracy, acts of terrorism and the like. The Bimco form, for example, provides very general language as follows:

Neither the Owners nor the Charterers shall be responsible for any loss or damage or delay or failure in performance under this Charter Party resulting from Act of God, war, civil commotion, quarantine, strikes, lockouts, arrest or restraint of princes, rulers and peoples or any other event whatsoever which cannot be avoided or guarded against.

While the foregoing Bimco form deals with terrorism in terms of war risks, and requires written consent for the vessel to be ordered to an area involving such risk, there is no harm in providing further specifics, particularly in light of the current uncertainties regarding the definitions of “piracy” and “terrorism.” Contract terms are particularly important in view of

---

11 In re Tradex Internacional S.A., 1973 AMC 1609 (Arb. at NY 1973)(notice of readiness provided but no loading had commenced).
12 2005 AMC 2601 (SDNY 2005).
14 Id., Cl. 23, War.
the potential for exclusion of piracy and terrorism from hull coverage.\textsuperscript{11} Suffice it to say there have been reported piracy attempts on tug and barge operations.\textsuperscript{12}

The same force majeure analysis from other cases is applicable to hijacking and piracy issues. The \textit{Anvil Knitwear} decision discussed above, which involved an exclusion of cargo loss due to hijacking, found no involvement of the carrier. While a vessel should not be considered a specifically, foreseeable target to the same extent that a defined geographic area is forecast as the likely path of a hurricane, there are destinations that are considered at risk,\textsuperscript{13} and in any event, the traditional force majeure case law would necessarily be invoked by adverse parties to require a showing that reasonable precautions were in effect. The defense could therefore be at risk in the absence of the ability to make a showing of a security plan and crew training.\textsuperscript{14}

\textbf{XVI

CONCLUSION}

The application of a successful defense based on force majeure or Act of God necessarily focuses on human factors. The defense may be lost by a showing that actions of the party asserting the defense contributed to the casualty, or that notwithstanding acts of nature of exceptional magnitude, the loss could have been avoided by exercise of reasonable care, or adequate precautions. Mitigating factors and reasonableness of actions taken are also taken into account in decisions evaluating intervention of governmental authorities, acts of third parties, or other events beyond the control of the parties. While the careful practitioner will necessarily plead force majeure as an affirmative defense, the practical application of the doctrine is, essentially, a showing of due care, contingency planning and precautionary measures, lack of negligence, and reasonable conduct.

\textsuperscript{11}For renewal the majority of underwriters are requiring the piracy peril to be deleted from the hull policies and added to the war risk policies.” Marsh, “Marine Market Monitor,” p. 3 (July 2009).

\textsuperscript{12}Singapore Information Fusion Centre description of April 5, 2009 pirate hijacking of anchoring Tug Prospa T1 with an empty barge in tow. \url{http://www.recaap.org/incidentpdf/incident2009/IncidentAlert%207%20Apr%2009.pdf}

\textsuperscript{13}The International Maritime Bureau Piracy Reporting Centre provides an online database of at risk areas. See, e.g., the IMB Live Piracy Map, \url{http://www.iccbs.org/index.php?option=com_fabrik&view=visualization\&controller=visualization\&GoogleMap\&Itemid=219}.

\textsuperscript{14}Summary information on Anti Piracy measures and a security plan is provided in the U.S. Coast Guard Port Security Advisory 10-09, and Supplementary Advisory 11-09.
EDITORIAL BOARD

Jane Andrawortha
Clyde & Co, LLP
London

James W. Bartlett, III
Semmes Bowen & Semmes, PC
Baltimore

Prof. David J. Bederman
Emory University

Prof. Francesco Berlingieri
President of Honour
Comité Maritime International
Genoa

John A.C. Cartner
Cartner & Fiske, L.L.C.
Washington, D.C.

Michael Marks Cohen
Nicoletti, Hornig & Sweeney
New York City

Prof. Martin Davies
Tulane University

Danièle Dion
Brison Bishop
Montreal

Prof. Steven F. Friedell
Rutgers University

Edgar Gold, Q.C.
The Nautical Institute (Qld)
Brisbane, Australia

Hon. Charles S. Haight, Jr.
United States District Court
Southern District of New York

Hon. Alex T. Howard, Jr.
United States District Court
Southern District of Alabama

Prof. Robert M. Jarvis
Nova Southeastern University

John D. Kimball
Blank Rome, LLP
New York City

Hon. Ronald R. Lagueux
United States District Court
District of Rhode Island

Warren J. Marwedel
Marwedel Minichello & Reeb
Chicago

Bruce A. McAllister
Alley, Mans, Rogers & Lindsay, P.A.
Palm Beach

John P. McMahon
McMahon & Connell, P.C.
Rock Hill, SC

Constantine G. Papavizas
Winston & Strawn
Washington, DC

Prof. David W. Robertson
University of Texas

Prof. George A. Rutherglen
University of Virginia

Richard F. Southcott
Stewart McKeIvey Stirling, Scales
Halifax, NS

Graydon S. Staring
Nixon Peabody
San Francisco

Douglas B. Stevenson
Scamman’s Church Institute
New York City

Prof. Joseph C. Sweeney
Fordham University

Prof. William Tetley
McGill University

Dr. Michael W. D. White
University of Queensland

Dr. Frank L. Wiswall, Jr.
Caxine, ME