I want to begin in talking about National Security issues on the horizon and emerging threats in cyber security by talking first and foremost about what it means to talk about Homeland Security. What does it mean to talk about homeland security? It may not be what you think it is. Everybody’s heard of it. Not everybody knows what it means we do, or when we say we have a secure homeland. So I want to discuss cyber security from a homeland security perspective, and for this to make sense I have to tell you how homeland security differs from national security. Because it’s striking to me how different is. Homeland security really is a different cat than national security.

And from this lens of homeland security I will talk about cyber security and reflect on what is the biggest problem we collectively face as Cyber Sun rises, and it is rising. I’ll close with a few reflections on what I think we’ve learned in homeland security in the past 10 years since 9-11 and how those lessons will guide us here.

Ok, so what is Homeland Security?

When the administration came into office in 2009, the department was 5 years old. What I used to tell people and what I tell them today is that we’re 8.5 years old and that that’s good news. We’re not 1 year old for the eighth time. I’ve been in organizations like that; maybe some of you have as well. You can tell the difference instantly.

10 years after 9-11, again we have all kinds of name recognition but we do not have the kind of understanding we should. What’s the vision? Andy Goodpaster said to me once, “If you don’t know where you’re going you’re not going to get there.” The sentence is: Have a safe, secure, resilient place where the American way of life can thrive. There is a lot that goes into it, but we think we know how to prioritize the most important things.

We need to prevent another 9-11. Prevent another terrorist attack. We need to secure our borders, manage them effectively. We need to administer and manage our immigration laws, ensure our cyber security and build national resilience. Let me tell you a little bit about what this takes. What does this mean we do? Not at the end of the day, but at the beginning of the day. What do nearly a quarter million employees do every day when they wake up devoted to homeland security?

First and foremost to prevent terrorism we need to understand the threat. Know where the threat is coming from, know why. Prevent access of threat actors to the most dangerous weapons of mass destruction, and reduce vulnerabilities as a nation, particularly to critical infrastructure.

If we are going to secure borders and manage our borders you can begin to see the duality of homeland security. On the one hand we want to keep out people and goods that might be dangerous but we want to expedite legitimate trade and travel. None of this facilitate stuff. We want to expedite legitimate trade and travel while at the same time keeping out people and goods that might be dangerous.

Similarly, if we are going to enforce our immigration laws, we are resting on a fundamental right that every country has to know who lives and works within our borders. Here too there is a duality you can see. On the one hand you want to keep out people who might be dangerous, but on the other hand, as I can attest to as the grandchild of immigrants; we want to welcome those who enrich our culture and our economy. And we do it every day. There is nothing quite like looking freedom in the face when you see
new immigrants, new American citizens take the oath of allegiance to this country. It’s an extraordinary experience if you haven’t had a chance to do it. That’s our privilege.

We need to safeguard and secure cyber space. This is a new mission that we’ve called out and we’ll talk about why it’s important in homeland security. Because people have asked us, cyber space, really? Really? Really. Really, cyber space. Did you wake up this morning? Did you turn on the radio? Did you get that coffee maker to work? Did you get an e-mail, did you send one? Did you make a phone call? You’ve touched cyber space more than you know before 8 a.m.

How do we secure and safeguard cyber space? Again, by preventing attacks and protecting vital infrastructure but it is not enough to do that. We need to build an open and secure cyber ecosystem and I’ll talk a little about that.

And finally we think that among our priorities in homeland security we need to build national resilience. What does that mean we do? Mitigate hazards; ensure our preparedness; have responsive emergency services; rapid recovery.

How do we do that? We do that by beginning with empowered individuals. People who have the information they need and can act on that information. I can tell you from a long period in my adult life dealing with international crises we respond in the first instance to a crisis with food and water and shelter and security and we think those items are important, and they are … but I can tell you that information is equally important. It is a commodity in a crisis, particularly when you are initially responding. If you don’t have an informed population, you don’t have a stable population. Information is essential. So building national resilience first and foremost begins with empowered individuals who know what you know and know what to do about it.

We need to build capable communities and a responsive federal system. The Federal government can’t do everything in a crisis. Feds are not best first responders; even local officials are not the best first responders. The best first responders in many cases are locals. We need empowered individuals, capable communities and a responsive federal system to build national resilience.

What does it mean to have a Homeland Security perspective on securing cyberspace?

I told you I would give you my reflections on how homeland security differs from national security, and I’ve been doing national security for a long time.

National security is strategic, it’s centralized, it’s top-driven. Homeland security is operational, it’s transactional, it’s decentralized, it’s bottom-driven. It’s driven by the grassroots of this country, by the states, by the municipalities, by the cities and towns that experience these issues first-hand, day-to-day. It’s driven by the nearly two million people that pass through the TSA systems every day – every day, pass through these systems.

We have global connections in this country, and we manage them in a transactional way, in an operational way, in homeland security. So unlike National Security – strategic, centralized, top-driven; it’s about all of us – homeland security is operational, decentralized, bottom-driven; it’s about each of us.

The national security culture has very strong influences from the military, the intelligence community. Homeland security, it is law enforcement, emergency management, and the political environment that’s the vibrancy of this country.
In national security there is a culture of confidentiality, the need to protect the nation’s most sensitive information. In homeland security there is an expectation of transparency: it’s not a need to know, it’s a duty to share, it’s an expectation to share.

In national security there’s unity of command. In homeland security, it’s a unity of effort.

It’s a different model. It’s a different model. And we need to understand the things that we deal with from the differences that that model represents. Homeland security of course is a part of national security, but it’s different.

So with this as a backdrop, we turn to cyber space. How vulnerable are we? How high can you go. We are very vulnerable. Terabytes of information are stolen, government secrets, industry blueprints, data of all kinds, identities. The threat is very real but a little capability can go a long way. Offense usually wins. The threat is proximate. The threat is consequential, and frankly, we are past the point of planning – we need to do something.

Despite all those billions in all that time, not one significant cyber problem has been solved. You cannot access, transit, stop, or shop anywhere on the internet confident that your identity and information will not be subject to some challenge or compromise.

What do we need to protect against? Villains, thieves, scoundrels, international criminal gangs, and nation states: they steal our information and use it against us to distort our own identities and compromise our future opportunities. The status quo is not acceptable. Whether it is government seeking strategic advantage, or sophisticated international criminal networks that move people, money, drugs, and weapons, they are smart and well resourced and some say they are robbing us blind.

Why does this matter? This country runs on the internet but cyberspace is a domain unlike any other. People are searching for a metaphor or an analogy. I leave it to the better minds, as I said every ladder has a bottom rung. Cyberspace is the endoskeleton, the very endoskeleton of modern life. And securing cyber space requires hard work and has no shortcuts. We have to improve quality, security, agility of our systems, networks, processes, and we have to use every capability that this nation has to offer, every skill at our disposal.

What does this mean? We all have a role to play, from individual users who must practice key cyber hygiene and stay current on what those measures are. It can feel impossible today to know what will secure you in cyberspace. Nevertheless, individuals must be empowered. We need to take advantage of password protected regimes, firewalls and other mechanisms, but they must get easier to use. The only way to inoculate is to not connect, and that is not an option.

Industry must continue to innovate. It is the genius of American companies and minds that brought us the internet and has expanded its potential to ways we couldn’t imagine a few years ago. So it must be the genius of American companies to find a way to provide security while providing value.

What needs doing? Everything. Security has to be built in, not added on later. Products should be shipped with security already activated, not sitting inert. Supply chains must be devised in ways that reduce the risk of product corruption or diversion. Critical infrastructure providers have to adopt security measures to counter threats and reduce vulnerabilities.

What does this mean? IT systems management; we must know and train our users, know who is on the net, and know what they have access to. Know and protect our systems, technology, networks, and know their boundaries.
Can individuals on their own behalf or the market do it? Some say let the market respond. The market had a few opportunities; there have been a few large intrusions. The market barely noticed. We can’t rely simply on the market. We can’t leave it to individuals to simply find their own way. We need all the resources of this government, all the resources this nation has to offer, and deploy them, in the service of cyber security.

What role is there for government? A few things have impressed me on this question. The first thing I noticed is that technology is moving too fast. It’s just really trending out of our grasp. Now this is ironic because technology is the word invented to describe tools, things which are within our grasp. Technology is too far out in front of us. We can’t reach it. We’re not leaving this to the experts; we leave this to the next generation. How many of us ask our kids to “turn this on” or “how do I get rid of this stuff on my screen?” Thank God for them. We’re not leaving this to the experts; we leave this to the next generation. The problems we will be facing, the solutions to these problems even two years from now have not been invented yet. That’s how fast technology is moving.

Second is that we’re slow to adapt. The social adaptation to the advantages, and the promise, and dangers of technology, we’re not keeping up and law is a lagging indicator. The law is a lagging indicator. So we have technology way out in front, we’ve got society somewhere in the middle, and we’ve got the law trailing behind. This is striking. Over the course of time, over the course of my adult lifetime is a convergence of social and political norms that are very powerful and very powerfully operating among societies today and these are the norms and expectations that people have of transparency, inclusivity and reciprocity.

What do I mean? People expect to know what’s going on, even if it doesn’t concern them. They expect to be included in every walk of life. “Nothing about me without me.” Ask yourself: Do you think things are legitimate if you didn’t know about them? No, you don’t. And reciprocity; if it’s good enough for me, it’s good enough for you, and vice versa. Inclusivity, transparency and reciprocity are adding up to a very powerful norm of accountability running in all directions: Not only are our governments to us, but governments to each other, and ourselves to each other. People are more mobile, educated and healthier. This means informative acting on what they know.

What does this mean? People are more informed and more active in what they know. We see social discontent in this country like the Occupy movement, or social discontent in Europe. My colleagues and I have traveled to Europe more than a dozen times to negotiate a data sharing arrangement with the Europeans. People are angry. People are angry. But it’s born of fear, not purpose. And that fear stems from a basic realization that we have lost the ability to institutionalize trust.

What institutions do we feel we can trust today? People say they can’t trust the market, or media, banks, religious institutions, governments, education institutions; we’ve lost the ability to institutionalize trust! Really!

What are the attributes of institutions that we do trust, what can we say about them? We know very clearly their value proposition: a clear source of expertise and responsiveness. In other words, there is performance with predictability and we know we can see the boundaries with these institutions. That means they have a certain humility about the role they are playing in our lives. The best institutions tell us what they’re doing and why. Not always how – they are leaving that increasingly to us, to help figure that out. I happen to live in a household that operates under that golden rule; you get to tell me what to do or how to do it, but not both. It’s a recipe for success, it works. Is that “the what” or “the how”?
But the very best institutions tell us what and why, because people are smart, switched on, involved, they care. We see transparency, inclusivity, accountability; for none of these things do we have to sacrifice decisiveness or the ability to set priorities.

What does this mean for homeland security and the challenges of cyber security? I’ll reflect for just a moment on the lessons over the last 10 years, since 9-11.

First, the world is still a dangerous place. Terrorism is still a persistent menace, even with Osama Bin Laden dead. But just as Capone’s death didn’t herald the death of crime, doesn’t mean Bin Laden’s death is the end of terrorism. Al-Qaida is still a source of direction for many, and we must tackle this head-on.

This country can protect us, we’ve learned this. We fight terrorism abroad through a combination of intelligence and information sharing, our military certainly, collaboration with trusted friends and allies. We fight terrorists domestically using our border tools, using law enforcement, not just federal assets, but 800,000 men and women at the State and Local level who protect communities. We fight with information sharing and learning from what we’ve seen abroad, and we fight it with the great American public.

What does that mean; it’s the third thing we’ve learned. We all have a role to play. So to speak of a secure homeland certainly is to speak of a freedom from fear, but also how we have come together as a nation, to secure our opportunities, freedoms, values, and principles, with creativity, fortitude, and resolve. These are the characteristics of every American you know, and I know, these are the characteristics of our spirit, and our culture, the American way of life that we’ve known all our lives.

Part of our national character is our national resilience. Disaster can strike, crises, without warning, with grave consequences, but we have learned a lot about preparedness and response. The public is an asset, keep them informed, engage local authorities quickly and early, be present and visible at the earliest signs of trouble, identify what must be done first, then do it fast and big, be clear about who is responsible for what, and give people a place to go for more help if needed. We’ve had a lot of disasters these last 10 years, but we’ve gotten beyond each one. It’s been hard and expensive and very heartbreaking, but we’ve recovered.

What does this tell us about cyber security? What we can do, what lies ahead, what will it take to keep us safe, in a world where people fly planes into buildings, stick bombs into shoes, and wire children to explode, where we live in an age when we know before victims do that there will be victims? How do we secure ourselves, our livelihoods, our interactions with the rest of the world when determined criminals, terrorists, and networks wake up every day with the sole purpose of undermining our laws, exploiting our weaknesses, stealing us blind, and trying to scare us to death?

Can we possibly protect ourselves; can we trust our institutions and our government? The answer is certainly yes. We can protect ourselves, we can trust each other, we can defeat terrorists who threaten us, rebuild when hurricanes strike, check advances of global disease, and restore the environment when disaster occurs. Just as we have overcome crises in the past, so now we have to set aside our differences, roll up our sleeves, and get down to work, harness our technology and put ourselves to the task that we can have an internet – a cyberspace – that is secure and open. The aim is confidence, not control.

But no actor can do all that needs doing. We need to build a cyber ecosystem where people and technology, supported by appropriate far sighted policies, bring all our capabilities together; so that we can detect intrusions, respond with speed, and recover in full. We need consensually-driven rule-based regimes where roles and responsibilities are clear for all users: rules that set outcomes, not means; rules
that protect our most vulnerable, and allow room for innovation; clear, fair, broadly supported, and extensible internationally.

The ecosystem will not just be about law, but about behavior and norms - and so how about voluntary, interoperable, privacy enhancing authentication as a step of profound change? The internet itself operates on trust.

What’s the challenge: that as the cyber sun rises we will lose faith in each other? Not me. My greatest faith is in the American people, in this homeland. We built it based on trust, not distrust. Why do I have this faith? We have come so far together. If you know anyone in their 20’s, and that is a lot of you in this room, I’m pleased to say, we can only imagine how far we have to go, they are really and truly the greatest generation. I say to you, recognizing the gifts my parents gave me, the young people we have in this country, and they are truly the greatest generation.

So I’m placing my trust in them, in you, in all of us, in the American people, we will be able to build a safe secure resilient place where the American way of life can thrive. God bless us all. Thanks very much.