AMERICAN BAR ASSOCIATION

CYBERSECURITY LEGAL TASK FORCE

REPORT TO THE BOARD OF GOVERNORS

RESOLUTION

RESOLVED, That the American Bar Association urges the Executive and Legislative branches to consider the following guiding principles throughout the decision-making process when making U.S. policy determinations to improve cybersecurity for the U.S. public and private sectors:

Principle 1: Public-private frameworks are essential to successfully protect United States assets, infrastructure, and economic interests from cybersecurity attacks.

Principle 2: Robust information sharing and collaboration between government agencies and private industry are necessary to manage global cyber risks.

Principle 3: Legal and policy environments must be modernized to stay ahead of or, at a minimum, keep pace with technological advancements.

Principle 4: Privacy and civil liberties must remain a priority when developing cybersecurity law and policy.

Principle 5: Training, education, and workforce development of government and corporate senior leadership, technical operators, and lawyers require adequate investment and resourcing in cybersecurity to be successful.

REPORT

The American Bar Association recognizes the increasingly critical need for action in response to growing cybersecurity attacks against U.S. public and private sector entities that threaten the delivery of essential citizen services, security of corporate data, including intellectual property and trade secrets, U.S. government assets and data, and personally identifiable information of citizens. Widespread use of the Internet and information technology during the past decade has created unprecedented opportunities. New and innovative uses of the Internet and information technology have improved the delivery of essential goods and services, increased the quality of life, offer new ways to connect with citizens, and paved the way for economic growth across the globe. However, along with exciting new functionality, use of the Internet and information technology may introduce opportunities for criminals, terrorists, and nation states to undermine the delivery of these extraordinary capabilities and create national and economic security risks.

In this environment, the cybersecurity of our digital infrastructure is a national priority for leaders in both public and private sectors. The American Bar Association has a central role to play in promoting cybersecurity. The American Bar Association should provide the leadership and expertise for lawyers to gain, and remain, competent in cybersecurity and to protect client information from cybersecurity breaches. In addition, the American Bar Association should lead a new national dialogue on cybersecurity amongst the legal profession, as lawyers are actively counseling government, private corporations, and the non-profit communities. Legal scholars are similarly positioned in academia to lead discussions on evolving cybersecurity challenges and, more profoundly, to offer legal and policy solutions to resolve complex new challenges. Finally, the American Bar Association should promote policy principles that advance our national agenda toward greater security and privacy protections, at home and abroad.

This report provides an overview of cyber threats, shared risks, and new roles and responsibilities for leaders in the government, corporations, legal profession, academia, and citizenry. The report concludes with five initial principles to guide the private sector and the executive and legislative branches of government in developing cybersecurity policies and working with leaders in both the public and private sectors.

Cyber Threat Environment

Sophisticated cybersecurity threats are increasingly targeting both citizen information and critical economic and national security assets. Global threats from criminals, terrorists, and nation states pose significant risks to critical infrastructure, government and corporate data, personally identifiable information, and intellectual property creating concerns in the areas of consumer protection, privacy and critical infrastructure protection.[1] Cyber crimes are not just a threat to information systems, but also, in the hands of an anarchist, a terrorist or a hostile group or nation to tangible assets, communications necessary for a functioning society, political processes such as elections, and human life.

Both government and the private sector have demonstrated a concern for cybersecurity threats, risks, and their potential consequences, as demonstrated by significant government and private sector investments in cybersecurity infrastructure. However, resource commitments alone have not led to a comprehensive mitigation of cybersecurity vulnerabilities. Rather, the nation is facing risks that demand new ways of thinking and expertise to address them.

Shared Risks

Cybersecurity threats equally target both the public and private sectors. Public and private sectors also share common vulnerabilities, such as reliance on the global Internet and use of modern technologies to reach customers and citizens across the globe. As a result, cybersecurity presents both shared risks and shared responsibilities requiring the public and private sectors to address risks separately and in partnership.

National leaders have treated cybersecurity and collaboration as a national priority and a shared public-private responsibility for well over a decade. Presidential Decision Directive 63, signed in1998, formalized public-private partnerships as a key part of the nation's first cybersecurity policy.[2] Since then, successive Administrations have uniformly adopted a collaborative approach for managing cybersecurity. Similarly,

---

[1] The 2012 Verizon Data Breach Investigations annual report examined 855 data breach incidents from 2011 and found that those incidents alone led to 174 million compromised records. Verizon, *2012 Data Breach Investigations Report, available at* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf, (last visited 25 September 2012). Also in 2011, the Department of Homeland Security noticed a 383 percent increase in attacks on critical infrastructures. Federal Times, *Report: Cyber attacks on critical infrastructure jump 383% in 2011, available at* http://www.federaltimes.com/article/20120703/IT01/307030004/Report-Cyber-attacks-critical-infrastructure-jump-383-2011, (last visited 25 September 2012). *Foreign Spies Stealing US Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage*, 2009-2011; Office of the National Counterintelligence Executive, (October 2011); www.ncix.gov

[2] Presidential Decision Directive 63, Critical Infrastructure Protection (May 1998). Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection (2003); Comprehensive National Cybersecurity Initiative, National Security Presidential Directive 54/ Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) (2008); Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure (2009).

leaders in the private sector and academia have also recognized the value of public-private collaboration as a strategic priority. Multiple findings from the nation's leading academic institutions, think tanks, and trade associations call for new levels of collaboration around shared cybersecurity risks.

New Roles, New Responsibilities

The nation requires new and unprecedented levels of public-private collaboration. Effective frameworks will demand a rethinking of current roles and responsibilities across affected stakeholders in several areas.

- The U.S. government must protect citizen data as well as unclassified and classified systems. In addition, the U.S. government needs to leverage its resources across civilian, law enforcement, defense, intelligence, and diplomatic components to share threat information and collaborate with the private sector.

- Private sector companies that store or process citizen data, or own and operate critical infrastructures, should continue to promote effective, company-specific security measures, as well as participate with the government in collaborative efforts to address shared cybersecurity threats.

- Lawyers have a deep responsibility (i) to protect client information and to develop, and maintain secure systems, (ii) to play an active role in the creation and implementation of public-private frameworks, and (iii) to represent clients that may have fallen victim to cybercrime.

- Academia should continue to participate in a national dialogue on law, policy, and technological innovations. Legal scholars, law school administrators, and others in the legal community should foster an environment in which law students can undertake future leadership roles and responsibilities relating to cybersecurity.

- Consumers and citizens also have unique roles and responsibilities, and they need improved resources to help them counter and prevent cybersecurity risks.

National Policy Principles

Cybersecurity is a complex issue that requires a holistic approach to address current and future risks. The American Bar Association should play a leadership role in preparing lawyers to contribute to this multidisciplinary discussion and also be prepared to contribute to the national dialogue on cybersecurity. Toward those ends, the American Bar Association should adopt the following initial principles to guide its leadership role in the cybersecurity debate:

> **Principle 1:** Public-private frameworks are essential to successfully protect United States assets, infrastructure, and economic interests from cybersecurity attacks.

Comment: Advancing cybersecurity at home and abroad will require solutions that address both public and private sector risks. Frameworks must be developed to define new roles and responsibilities for all of the participants who are necessary to secure cybersecurity. These include governments at all levels, corporations, nonprofit organizations, non-governmental organizations (NGOs), lawyers, academics, and citizens. These diverse groups must be molded into workable frameworks that facilitate cooperation and effectively confront cybersecurity threats. New partnership frameworks to address more virulent cyber threats need to be analyzed and existing, effective partnership frameworks should have continued support and participation.

> **Principle 2:** Robust information sharing and collaboration between government agencies and private industry are necessary to manage global cyber risks.

Comment: In light of the global nature of shared cybersecurity threats, advanced forms of information sharing and collaboration are needed. Information on threats is necessary, but it is not nearly sufficient to counter the risks. Public and private sectors need to share not only information on threats, but also knowledge on how to manage cybersecurity threats, including effective tools, practices, and risk frameworks. The public and private sectors should engage in a continuing dialogue to better enable them to constantly share information on new capabilities, risks, and developments and how to react to them, while still maintaining privacy and civil liberty protections.

> **Principle 3:** Legal and policy environments must be modernized to stay ahead of or, at a minimum, keep pace with technological advancements.

Comment: Effective public-private frameworks for information sharing and collaboration will require the modernization of law and policy. At a minimum, the public and private sectors should review and consider measures that remove impediments to greater public-private collaboration and the sharing of capabilities. The ability to track and trace cybercriminal activity and legal issues pertaining to liability, antitrust, and the protection of government and corporate information remain legal challenges that should continue to be reviewed and considered. The legal, engineering, computer, and scientific academies should support rigorous review of legal doctrines and application of those doctrines, and offer innovative solutions for helping to create an effective legal and policy environment for the coming decade.

> **Principle 4:** Privacy and civil liberties must remain a priority when developing cybersecurity law and policy.

Comment: Privacy and civil liberties must remain bedrock principles as the nation grapples with complex cyber threats and global attacks. Lawmakers have both a responsibility to foster new forms of collaboration, but also to protect and maximize privacy and civil liberties as part of these solutions. Since cybersecurity programs will traffic in digital information that could contain sensitive personal information or reflect constitutionally protected activity, it is crucial that these principles are fundamentally

built into cyber programs from the start, and that cyber programs be conducted with reasonable accountability. Furthermore, the legal profession has a unique role to play in educating lawmakers and the public as to the choices that are available, the impact of those choices, and the challenges associated with balancing cybersecurity needs against privacy and civil liberties rights.

> **Principle 5:** Training, education, and workforce development of government and corporate senior leadership, technical operators, and lawyers require adequate investment and resourcing in cybersecurity to be successful.

Comment: New public-private frameworks for cybersecurity will require a trained and supportive workforce to implement and maintain them. The nation requires a focus on developing cybersecurity expertise within all levels of the government and private sector and within the general population. The ABA should have a critical role in educating and encouraging lawyers, law firms, and citizens about the need to act to minimize cyber security risks. The weakest link may be the individual's home computer that has been infected and is serving a proxy role in cybercriminal activity. Lawyers must dedicate themselves to continually developing the competencies necessary to effectively secure client and firm data and systems and participate in cybersecurity initiatives with the government, corporations, the legal profession, academia, and citizens.

GENERAL INFORMATION FORM

Submitting Entity: CYBERSECURITY LEGAL TASK FORCE

Submitted By: JUDITH MILLER AND HARVEY RISHIKOF, CO-CHAIRS

1. Summary of Resolution(s).

Sophisticated cybersecurity threats are increasingly targeting citizen information as well as critical economic and national security assets. Consequently, the cybersecurity of our digital infrastructure is a national priority for leaders in both public and private sectors. In order to effectively engage in the ongoing national dialogue regarding cybersecurity, the Resolution establishes American Bar Association guiding principles for the Executive and Legislative branches to consider when making U.S. public policy determinations to improve cybersecurity.

2. Approval by Submitting Entity. OCTOBER 10, 2012

3. Has this or a similar resolution been submitted to the House or Board previously?
NO

4. What existing Association policies are relevant to this Resolution and how would they be affected by its adoption? Nothing on this subject at this time.

5. What urgency exists which requires action at this meeting of the House? Cyber terrorism is an extremely serious threat to our nation's security. The danger is real, its present and its growing. In a speech to business executives on October 11, Defense Secretary Leon Panetta admitted that the computer virus that attacked the Mideast energy companies over the summer was 'the most destructive cyberattack on the private sector to date.' The ABA ideally should be in a position to provide comments to U.S. decisionmakers as they consider public policy to improve cybersecurity. While Congress is considering legislation, the White House is also considering issuing an Executive Order. Timing is of the essence. President Bellows spoke of the need for the Association to weigh in on cyber issues during her address to the ABA House of Delegates when she was sworn in as ABA president. The cyber crisis is redefining how we think about security, crime and intellectual property; in one sense the concept of struggle and competition is moving from the war room to the boardroom. This cannot wait until February if the Association is to comment on these pressing issues.

6. Status of Legislation. (If applicable) Cyber legislation is stalled at this time; the President is considering issuing an Executive Order. Given growing cybersecurity threats, Congress and the Administration can act at any time.

7. Brief explanation regarding plans for implementation of the policy, if adopted by the House of Delegates. The principles will provide the Association the opportunity to engage in discussions regarding cybersecurity. Cybersecurity issues have increasingly been the focus of hearings and consideration in both the executive and legislative branches, and also in the private sector.

8. Cost to the Association. (Both direct and indirect costs) none

9. Disclosure of Interest. (If applicable) to our knowledge , no conflicts of interest

10. Referrals. The Board of Governors approved the creation of the Task Force on Cybersecurity on June 1, 2012. This Task Force includes representatives from all ABA entities with an interest in cybersecurity and privacy. All relevant ABA entities having an interest or involvement in cybersecurity issues have been notified and their comments and suggestions have been incorporated into this report.

11. Contact Name and Address Information. (Prior to the meeting. Please include name, address, telephone number and e-mail address) Harvey Rishikof – 202-288-2013 or Judith Miller – 202-341-8127

12. Contact Name and Address Information. (Who will present the report to the House? Please include name, address, telephone number, cell phone number and e-mail address.)

Allen Goolsby, Hunton & Williams LLP, 951 E. Byrd Street, Richmond, VA 23219 – phone: 804-788-8289; agoolsby@hunton.com and

Tim Bouch, Leath, Bouch & Seekings LLP, 92 Broad St, Charlottesville, SC 29401 - phone: 843-937-8811; tbouch@leathbouchlaw.com

EXECUTIVE SUMMARY

1. Summary of the Resolution

Sophisticated cybersecurity threats are increasingly targeting citizen information as well as critical economic and national security assets. Consequently, the cybersecurity of our digital infrastructure is a national priority for leaders in both public and private sectors. In order to effectively engage in the ongoing national dialogue regarding cybersecurity, the Resolution establishes American Bar Association guiding principles for the Executive and Legislative branches to consider when making U.S. public policy determinations to improve cybersecurity.

2. Summary of the Issue that the Resolution Addresses

Growing cybersecurity attacks against U.S. public and private sector entities threaten the delivery of essential citizen services, security of corporate data, including intellectual property and trade secrets, U.S. government assets and data, and personally identifiable information of citizens. As cybersecurity attacks have evolved, public and private sector leaders have been challenged to further more than decade-old policy foundations to effectively confront cybersecurity threats. With cybersecurity threats equally targeting the public and private sectors, legislation and policy must drive new and unprecedented levels of public-private collaboration across a large stakeholder group including all levels of government, corporations, the legal community, academia and citizenry.

Currently, Congress is considering several legislative solutions and the Administration is developing an Executive Order to improve the nation's cybersecurity preparedness. In this environment, the American Bar Association requires a policy position to weigh in on pressing cybersecurity issues.

3. Please Explain How the Proposed Policy Position will address the issue

The Resolution is designed to equip the American Bar Association with widely-supported guiding principles that will enable the Association to weigh in on cybersecurity legislation and policy in the short term. Over the long term, the guiding principles will provide a framework to drive the Association's continued focus on cybersecurity.

4. Summary of Minority Views

The Resolution is designed to encompass varying views on cybersecurity and present a framework to accommodate all stakeholders. Therefore, there are no known minority views at this time.