CYBERSPACE POLICY REVIEW

Assuring a Trusted and Resilient Information and Communications Infrastructure

Preface

Cyberspace touches practically everything and everyone. It provides a platform for innovation and prosperity and the means to improve general welfare around the globe. But with the broad reach of a loose and lightly regulated digital infrastructure, great risks threaten nations, private enterprises, and individual rights. The government has a responsibility to address these strategic vulnerabilities to ensure that the United States and its citizens, together with the larger community of nations, can realize the full potential of the information technology revolution.

The architecture of the Nation's digital infrastructure, based largely upon the Internet, is not secure or resilient. Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations. Our digital infrastructure has already suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive military information. Other intrusions threaten to damage portions of our critical infrastructure. These and other risks have the potential to undermine the Nation's confidence in the information systems that underlie our economic and national security interests.

The Federal government is not organized to address this growing problem effectively now or in the future. Responsibilities for cybersecurity are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way. The government needs to integrate competing interests to derive a holistic vision and plan to address the cybersecurity-related issues confronting the United States. The Nation needs to develop the policies, processes, people, and technology required to mitigate cybersecurity-related risks.

Information and communications networks are largely owned and operated by the private sector, both nationally and internationally. Thus, addressing network security issues requires a public-private partnership as well as international cooperation and norms. The United States needs a comprehensive framework to ensure coordinated response and recovery by the government, the private sector, and our allies to a significant incident or threat.

The United States needs to conduct a national dialogue on cybersecurity to develop more public awareness of the threat and risks and to ensure an integrated approach toward the Nation's need for security and the national commitment to privacy rights and civil liberties guaranteed by the Constitution and law.

Research on new approaches to achieving security and resiliency in information and communications infrastructures is insufficient. The government needs to increase investment in research that will help address cybersecurity vulnerabilities while also meeting our economic needs and national security requirements.

Executive Summary

The President directed a 60-day, comprehensive, "clean-slate" review to assess U.S. policies and structures for cybersecurity. Cybersecurity policy includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The scope does not include other information and communications policy unrelated to national security or securing the infrastructure. The review team of government cybersecurity experts engaged and received input from a broad cross-section of industry, academia, the civil liberties and privacy communities, State governments, international partners, and the Legislative and Executive Branches. This paper summarizes the review team's conclusions and outlines the beginning of the way forward towards a reliable, resilient, trustworthy digital infrastructure for the future.

The Nation is at a crossroads. The globally-interconnected digital information and communications infrastructure known as "cyberspace" underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security. This technology has transformed the global economy and connected people in ways never imagined. Yet, cybersecurity risks pose some of the most serious economic and national security challenges of the 21st Century. The digital infrastructure's architecture was driven more by considerations of interoperability and efficiency than of security. Consequently, a growing array of state and non-state actors are compromising, stealing, changing, or destroying information and could cause critical disruptions to U.S. systems. At the same time, traditional telecommunications and Internet networks continue to converge, and other infrastructure sectors are adopting the Internet as a primary means of interconnectivity. The United States faces the dual challenge of maintaining an environment that promotes efficiency, innovation, economic prosperity, and free trade while also promoting safety, security, civil liberties, and privacy rights.[1] It is the fundamental responsibility of our government to address strategic vulnerabilities in cyberspace and ensure that the United States and the world realize the full potential of the information technology revolution.

The status quo is no longer acceptable. The United States must signal to the world that it is serious about addressing this challenge with strong leadership and vision. Leadership should be elevated and strongly anchored within the White House to provide direction, coordinate action, and achieve results. In addition, federal leadership and accountability for cybersecurity should be strengthened. This approach requires clarifying the cybersecurity-related roles and responsibilities of federal departments and agencies while providing the policy, legal structures, and necessary coordination to empower them to perform their missions. While efforts over the past two years started key programs and made great strides by bridging previously disparate agency missions, they provide

[1] Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and 111th Congress, at 5.*

an incomplete solution. Moreover, this issue transcends the jurisdictional purview of individual departments and agencies because, although each agency has a unique contribution to make, no single agency has a broad enough perspective or authority to match the sweep of the problem.

The national dialogue on cybersecurity must begin today. The government, working with industry, should explain this challenge and discuss what the Nation can do to solve problems in a way that the American people can appreciate the need for action. People cannot value security without first understanding how much is at risk. Therefore, the Federal government should initiate a national public awareness and education campaign informed by previous successful campaigns. Further, similar to the period after the launch of the Sputnik satellite in October, 1957, the United States is in a global race that depends on mathematics and science skills. While we continue to boast the most positive environment for information technology firms in the world, the Nation should develop a workforce of U.S. citizens necessary to compete on a global level and sustain that position of leadership.

The United States cannot succeed in securing cyberspace if it works in isolation. The Federal government should enhance its partnership with the private sector. The public and private sectors' interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure. There are many ways in which the Federal government can work with the private sector, and these alternatives should be explored. The public-private partnership for cybersecurity must evolve to define clearly the nature of the relationship, including the roles and responsibilities of each of the partners.[2,3,4] The Federal government should examine existing public-private partnerships to optimize their capacity to identify priorities and enable efficient execution of concrete actions.[5,6,7]

The Nation also needs a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force. International norms are critical to establishing a secure and thriving digital infrastructure. In addition, differing national and regional laws and practices—such as laws concerning the investigation and prosecution of cybercrime; data preservation, protection, and privacy; and approaches for network defense and response to cyber attacks—present serious challenges to achieving a safe, secure, and resilient digital environment. Only by working with international partners can the United States best address these challenges, enhance cybersecurity, and reap the full benefits of the digital age.

The Federal government cannot entirely delegate or abrogate its role in securing the Nation from a cyber incident or accident. The Federal government has the responsibility to protect and defend the country, and all levels of government have the responsibility to ensure the safety and well-being of citizens. The private sector, however, designs, builds, owns, and operates most of the digital infrastructures that support government and private users alike. The United States needs a

[2] Written testimony of Scott Charney (Microsoft) to the House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, March 10, 2009, at 4.
[3] Cross-Sector Cyber Security Working Group (CSCSWG) Response to 60-day Cyber Review Questions, March 16, 2009, at 2.
[4] Information Technology & Communications Sector Coordinating Councils, March 20, 2009, at 2.
[5] Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*, December 2008, at 43.
[6] TechAmerica, Response to 60-Day Cyber Security Review, at 6.
[7] Business Software Alliance, *National Security & Homeland Security Councils Review of National Cyber Security Policy,* March 19, 2009, at Q3.

comprehensive framework to ensure a coordinated response by the Federal, State, local, and tribal governments, the private sector, and international allies to significant incidents. Implementation of this framework will require developing reporting thresholds, adaptable response and recovery plans, and the necessary coordination, information sharing, and incident reporting mechanisms needed for those plans to succeed. The government, working with key stakeholders, should design an effective mechanism to achieve a true common operating picture that integrates information from the government and the private sector and serves as the basis for informed and prioritized vulnerability mitigation efforts and incident response decisions.

Working with the private sector, performance and security objectives must be defined for the next-generation infrastructure. The United States should harness the full benefits of technology to address national economic needs and national security requirements. Federal policy should address requirements for national security, protection of intellectual property, and the availability and continuity of infrastructure, even when it is under attack by sophisticated adversaries. The Federal government through partnerships with the private sector and academia needs to articulate coordinated national information and communications infrastructure objectives. The government, working with State and local partners, should identify procurement strategies that will incentivize the market to make more secure products and services available to the public. Additional incentive mechanisms that the government should explore include adjustments to liability considerations (reduced liability in exchange for improved security or increased liability for the consequences of poor security), indemnification, tax incentives, and new regulatory requirements and compliance mechanisms.[8,9]

The White House must lead the way forward. The Nation's approach to cybersecurity over the past 15 years has failed to keep pace with the threat. We need to demonstrate abroad and at home that the United States takes cybersecurity-related issues, policies, and activities seriously. This requires White House leadership that draws upon the strength, advice, and ideas of the entire Nation.

The review recommends the near-term actions listed in Table 1.

[8] Jim Harper, *Government-Run Cyber Security? No, Thanks.*, Cato Institute, March 13, 2009.
[9] Internet Security Alliance, *Issue Area 3: Norms of Behavior—Hathaway Questions,* March 24, 2009, at 2, 4-7.

TABLE 1: NEAR-TERM ACTION PLAN
1. Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.
2. Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.
3. Designate cybersecurity as one of the President's key management priorities and establish performance metrics.
4. Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
5. Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government.
6. Initiate a national public awareness and education campaign to promote cybersecurity.
7. Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.
8. Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement
9. In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.
10. Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

Table of Contents

Preface i

Executive Summary iii

Table of Contents vii

Introduction 1

I. Leading from the Top 7

II. Building Capacity for a Digital Nation 13

III. Sharing Responsibility for Cybersecurity 17

IV. Creating Effective Information Sharing and Incident Response 23

V. Encouraging Innovation 31

VI. Action Plans 37

Appendix A: Bibliography A–1

Appendix B: Methodology B–1

Appendix C: Growth of Modern Communications Technology in the United States and Development of Supporting Legal and Regulatory Frameworks C–1

Introduction

What is Cyberspace?

National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) defines cyberspace as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.

The globally-interconnected digital information and communications infrastructure known as "cyberspace" underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security. Information technology has transformed the global economy and connected people and markets in ways never imagined. To realize the full benefits of the digital revolution, users must have confidence that sensitive information is secure, commerce is not compromised, and the infrastructure is not infiltrated. Nation-states also need confidence that the networks that support their national security and economic prosperity are safe and resilient. Achieving a trusted communications and information infrastructure will ensure that the United States achieves the full potential of the information technology revolution. The December 2008 report by the Commission on Cybersecurity for the 44th Presidency states the challenge plainly: "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration."[10]

Protecting cyberspace requires strong vision and leadership and will require changes in policies, technologies, education, and perhaps laws. Demonstrating commitment to cybersecurity-related issues at the highest levels of government, industry, and civil society will allow the United States to continue to lead innovation and adoption of cutting-edge technology, while enhancing national security and the global economy.

Case for Action

Threats to cyberspace pose one of the most serious economic and national security challenges of the 21st Century for the United States and our allies. A growing array of state and non-state actors such as terrorists and international criminal groups are targeting U.S. citizens, commerce, critical infrastructure, and government. These actors have the ability to compromise, steal, change, or completely destroy information.[11] The continued exploitation of information networks and the compromise of sensitive data, especially by nations, leave the United States vulnerable to the loss of economic competitiveness and the loss of the military's technological advantages. As the Director of National Intelligence (DNI) recently testified before Congress, "the growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and

[10] CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*, December 2008, at 11.
[11] Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee, Statement for the Record*, March 10, 2009, at 39.

other critical infrastructures." The Intelligence Community assesses that a number of nations already have the technical capability to conduct such attacks.[12]

The growing sophistication and breadth of criminal activity, along with the harm already caused by cyber incidents, highlight the potential for malicious activity in cyberspace to affect U.S. competitiveness, degrade privacy and civil liberties protections, undermine national security, or cause a general erosion of trust, or even cripple society. For example:

- ***Failure of critical infrastructures.*** CIA reports malicious activities against information technology systems have caused the disruption of electric power capabilities in multiple regions overseas, including a case that resulted in a multi-city power outage.[13]
- ***Exploiting global financial services.*** In November 2008, the compromised payment processors of an international bank permitted fraudulent transactions at more than 130 automated teller machines in 49 cities within a 30-minute period, according to press reports.[14] In another case reported by the media, a U.S. retailer in 2007 experienced data breaches and loss of personally identifiable information that compromised 45 million credit and debit cards.[15]
- ***Systemic loss of U.S. economic value.*** Industry estimates of losses from intellectual property to data theft in 2008 range as high as $1 trillion.[16]

Clean-Slate Review

Recognizing the challenges and opportunities, the President identified cybersecurity as one of the top priorities of his administration and directed an early 60-day, comprehensive review to assess U.S. policies and structures for cybersecurity. The review addressed all missions and activities associated with the information and communications infrastructure, including computer network defense, law enforcement investigations, military and intelligence activities, and the intersection thereof with information assurance, counterintelligence, counterterrorism, telecommunications policies, and

Cybersecurity policy as used in this document includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The scope does not include other information and communications policy unrelated to national security or securing the infrastructure.

[12] *Id.*, at 39-40.
[13] www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5, CIA presentation, SANS SCADA Security Summit, January 16, 2008.
[14] www.bankinfosecurity.com/article.php?art_id=1197, February 5, 2009.
[15] www.infoworld.com/d/security-central/retailer-tjx/reports-massive-data-breach-952, January 17, 2007.
[16] www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html. *See also* http://resources.mcafee.com/content/NAUnsecuredEconomiesReport, McAfee, "Unsecured Economies: Protecting Vital Information", January 2009. Projection based on survey by Purdue's Center for Education and Research in Information Assurance and Security.

general critical infrastructure protection. The review team of government cybersecurity experts inventoried relevant presidential policy directives, executive orders, national strategies, and studies from government advisory boards and private-sector entities. The review team solicited input from departments and agencies on their specific cybersecurity-related activities, authorities, and capabilities across these requirements and requested departments and agencies to identify any new or existing requirements that may not have been identified as part of the initial inventory. Scores of legal issues emerged, such as considerations related to the aggregation of authorities, what authorities are available for the government to protect privately owned critical infrastructure, the placement of Internet monitoring software, the use of automated attack detection and warning sensors, data sharing with third parties within the Federal government, and liability protections for the private sector.

The review team reached out to a wide array of stakeholders inside and outside the Federal government. The review team sought to be transparent by engaging a broad cross-section of industry, academia, the civil liberties and privacy communities, State governments, international partners, and the Legislative and Executive Branches to identify and assess other relevant programs and issues. Recognizing that there are opportunities for everyone—academia, industry, and government—to work together to build a trusted and resilient communications and information infrastructure, the review team engaged these stakeholders about the scope of the reviews and asked for input on pertinent areas of interest. The engagement process included more than 40 meetings and yielded more than 100 papers that provided specific recommendations and goals. Stakeholders' responses and public statements (e.g., Congressional testimony) helped to identify key requirements, illuminate policy gaps, suggest areas of improvement or collaboration, and frame the decision space for cybersecurity-related policies.

The review team found that throughout the evolution of the information and communications infrastructure, missions and authorities were vested with various departments and agencies by laws and policies enacted to govern aspects of what were then very diverse and discrete technologies and industries. The programs that evolved from those missions were focused on the particular issue or technology of the day and were not necessarily considered with the broad perspective needed to match today's sweeping digital dependence.

The impact of technology on national and economic security needs has led the Federal government to adapt by creating new laws and organizations. For example:

- In a 1918 Joint Resolution, Congress authorized the President to assume control of any telegraph system in the United States and operate it as needed for the duration of World War I.
- The Communications Act of 1934 formed the Federal Communications Commission (FCC) from the Federal Radio Commission and established a broad regulatory framework for all communications, by wire and radio, that has influenced the development of these technologies ever since.

- The Brooks Act of 1965 gave the National Bureau of Standards (NBS)—now the Department of Commerce's National Institute of Standards and Technology (NIST)—responsibilities for developing automatic data processing standards and guidelines pertaining to federal computer systems.
- In 1984, Executive Order 12472 re-chartered the National Communication System (NCS) as those telecommunication assets owned or leased by the Federal government that can meet U.S. national security and emergency preparedness needs. The Department of Homeland Security inherited the NCS in 2003.
- In 1994, through the Foreign Relations Authorization Act, the Department of State was delegated authority over foreign policy related to international communication and information policy.

Answering the question of "who is in charge" must address the distribution of statutory authorities and missions across departments and agencies. This is particularly the case as telecommunications and Internet-type networks converge and other infrastructure sectors adopt the Internet as a primary means of interconnectivity. Unifying mission responsibilities that evolved over more than a century will require the Federal government to clarify policies for cybersecurity and the cybersecurity-related roles and responsibilities of various departments and agencies. The review team analyzed responses from more than 20 federal departments and agencies and identified cybersecurity-related policy gaps, overlaps in mission areas, and opportunities to improve collaboration.

As the threats have grown in sophistication, efforts to address the risks of cyberspace and harmonize department and agency efforts have evolved over time as well. Presidential Decision Directive 63 (PDD-63), signed in May 1998, established a structure under White House leadership to coordinate the activities of designated lead departments and agencies, in partnership with their counterparts from the private sector, to "eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."[17] This policy was updated in 2003 with *The National Strategy to Secure Cyberspace.* It was further augmented later that year in Homeland Security Presidential Directive 7 (HSPD-7), which assigned the Secretary of Homeland Security the responsibility for coordinating the nation's overall critical infrastructure protection efforts, including for cyber infrastructure, across all sectors working in cooperation with designated sector-specific agencies within the Executive Branch.[18] Both of these policies focused purely on defensive strategies, and HSPD-7 did not encompass protection of Federal government information systems. In 2007, the Comprehensive National Cybersecurity Initiative (CNCI) took a different approach. Core to this strategy is the "bridging" of historically separate cyber defensive missions with law enforcement, intelligence, counterintelligence, and military capabilities to address the full spectrum of cyber threats from remote network intrusions and insider operations to supply chain vulnerabilities. The CNCI strategy was codified in NSPD-54/HSPD-23 and initiated programs focused

[17] Presidential Decision Directive 63, *Critical Infrastructure Protection,* May 22, 1998, at section II.
[18] Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection* (December 17, 2003). HSPD-7 also designated DHS as a the lead agency for the nation's Information Technology and Communications sectors, to share threat information, help assess vulnerabilities, and encourage appropriate protective action and the development of contingency plans.

primarily on the security of Executive Branch networks, which represent only a fraction of the global information and communications infrastructure on which the United States depends.

This paper summarizes the review team's findings and outlines initial areas of action to help the United States achieve a more reliable, resilient, and trustworthy digital infrastructure for the future. It does not provide an in-depth analysis of options or an extensive audit of programs. Instead, it presents the need for greater coordination and integrated development of policy. The paper structures the specific findings and options for action under five key topics: (1) leading from the top, (2) building capacity for a digital nation, (3) sharing responsibility for cybersecurity, (4) improving information sharing and incident response, and (5) building the architecture of the future. In addition, the paper is accompanied by appendices, including (A) a bibliography, (B) the study methodology, and (C) a brief history of modern communications technology.

I. Leading from the Top

Ensuring that cyberspace is sufficiently resilient and trustworthy to support U.S. goals of economic growth, civil liberties and privacy protections, national security, and the continued advancement of democratic institutions requires making cybersecurity a national priority. Accomplishing this critical and complex task will only be possible with leadership at the highest levels of government.

Anchor Leadership at the White House

Anchoring and elevating leadership for cybersecurity-related policies at the White House signals to the United States and the international community that we are serious about cybersecurity. Many departments and agencies as well as components of the Executive Office of the President (EOP) will need to harmonize disparate responsibilities and authorities to contribute effectively to cybersecurity. Currently, no single individual or entity has the responsibility to coordinate Federal government cybersecurity-related activities. Independent efforts will not be sufficient to address this challenge without a central coordination mechanism, an updated national strategy, an action plan developed and coordinated across the Executive Branch, and the support of Congress.

The Administration already has established an Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC), chaired by the National Security Council (NSC) and Homeland Security Council (HSC),[19] as the primary policy coordination body for issues related to achieving an assured, reliable, secure, and survivable global information and communications infrastructure and related capabilities.

The President should consider appointing a cybersecurity policy official at the White House, reporting to the NSC and dual-hatted with the NEC, to coordinate the Nation's cybersecurity-related policies and activities. This individual would chair the ICI-IPC and lead a strong process in consultation with other elements of the EOP to resolve competing priorities and coordinate interagency development of policies and strategies for cybersecurity.[20] The cybersecurity policy official should participate in all appropriate economic, counterterrorism, and science and technology policy discussions to inform them of cybersecurity perspectives.[21,22]

To be successful, the President's cybersecurity policy official must have clear presidential support, authority, and sufficient resources to operate effectively in policy formulation and the coordination of interagency cybersecurity-related activities. The cybersecurity policy official should be supported by at least two Senior Directors and appropriate staff from the NSC and at least one Senior Director and appropriate staff from the NEC. These directorates would report through the cybersecurity policy official and work together in pursuit of the goals set forth in this paper and established as national policy. In addition, to achieve additional scale and integration across the NSC, each NSC

[19] A separate 60-day study by the White House is examining the organizational structure of the two councils. The rest of the paper will refer just to the NSC for simplicity.
[20] CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*, December 2008, at 36-7.
[21] Written testimony of Scott Charney (Microsoft) to the House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, March 10, 2009, at 2.
[22] CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency,* December 2008, at 28.

regional and functional directorate should designate an individual to be responsible for following cybersecurity-related issues in the directorate's portfolio and coordinating with the directorate for cybersecurity.

The cybersecurity policy official should not have operational responsibility or authority, nor the authority to make policy unilaterally. Using interagency coordination processes, the cybersecurity policy official should harmonize cybersecurity-related policy and technology efforts across the Federal government, ensure that the President's budget reflects federal priorities for cybersecurity, and develop a legislative agenda, all in consultation with the Federal government's Chief Technology Officer and Chief Information Officer—along with the appropriate entities within the Office of Management and Budget (OMB), the Office of Science and Technology Policy (OSTP), and the NEC. [23]

This appointment also would make crisis management more effective by establishing the cybersecurity policy official as the White House action officer for cyber incident response (a similar role to the action officers who help the White House monitor terrorist attacks or natural disasters); departments and agencies would continue to perform their operational roles.

To facilitate coordination, all federal departments and agencies should establish a point-of-contact in their respective executive suites authorized to interface with the White House on cybersecurity-related issues.

The cybersecurity policy official—through the interagency policy development process—should prepare for the President's consideration an updated national strategy to secure the information and communications infrastructure. The strategy should include continued evaluation of CNCI activities and build, where appropriate, on its successes.[24] The national strategy should focus senior leadership attention and time toward resolving issues that hamper U.S. efforts to achieve an assured, reliable, secure, and resilient global information and communications infrastructure and related capabilities.[25] The strategy would assist government efforts to raise public awareness, renew and build international alliances and public-private partnerships, establish a more comprehensive national cyber response and recovery plan, and promote an aggressive research and development agenda that has the potential to result in new technologies that will enhance cybersecurity.

The Federal government should continue the principle of "mission bridging" started under the CNCI. Departments and agencies should expand the sharing of expertise, knowledge, and perspectives about threats, tradecraft, technology, and vulnerabilities between network defenders and the intelligence, military, and law enforcement organizations that develop U.S. operational capabilities in cyberspace. In addition, the cybersecurity policy official should help coordinate intelligence and military policies and strategies for cyberspace—including for countering terrorist use of the Internet—to ensure integration of all mission equities.The cybersecurity policy official should engage external advisory bodies. Many advisory bodies touch on cybersecurity-related issues, including the National Security and Telecommunications Advisory Committee (NSTAC), the

[23] Intelligence and National Security Association, *Critical Issues for Cyber Assurance Policy Reform,* at 3.
[24] CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency,* December 2008, at 59.
[25] Cross-Sector Cyber Security Working Group (CSCSWG) Response to 60-day Cyber Review Questions, March 16, 2009, at 11.

National Infrastructure Advisory Council (NIAC), the Critical Infrastructure Partnership Advisory Council (CIPAC), and the Information Security and Privacy Advisory Board (ISPAB). The cybersecurity policy official should review the responsibilities of these bodies and propose changes as necessary to optimize advice and eliminate unnecessary duplication.

Other structures will be needed to help ensure that civil liberties and privacy rights are protected. Such structures would signal transparency and build trust between the civil liberties and privacy community, the public, and the program for cybersecurity, especially if implemented from the outset.[26] It is important to reconstitute the Privacy and Civil Liberties Oversight Board (PCLOB), accelerate the selection process for its board members, and consider whether to seek legislative amendments to broaden its scope to include cybersecurity-related issues.[27] Other options include: facilitating regular engagement of government civil liberties and privacy advisors on policy matters for cybersecurity or designating a dedicated privacy and civil liberties officer within the NSC (or, more broadly, the EOP) to engage with the private-sector civil liberties and privacy community, an oversight board, and government civil liberties and privacy officers.[28, 29]

Equally important to developing cybersecurity policy, is assuring the effective execution and implementation of that policy to meet the goals of the larger strategy. Accordingly, the cybersecurity policy official, in consultation with OMB and other EOP entities, will need to ensure effective implementation of cybersecurity-related policy and activities. During the course of the 60-day review, stakeholders suggested a variety of options to coordinate and oversee cybersecurity activities. Several commentators identified strong executive leadership as well as focused, multi-year attention across the participating departments and agencies as critical elements to ensure that the U.S. Government has the mechanisms needed for an effective cybersecurity program. Currently, some of these oversight functions for existing cybersecurity efforts are being performed outside of the EOP. For example, the Joint Interagency Cyber Task Force (JIACTF), under the Director of National Intelligence, currently is responsible for coordinating and monitoring the implementation of the CNCI. The cybersecurity policy official, in consultation with OMB and other EOP entities, should develop structural options to perform appropriate oversight, implementation, and other functions. These could include among others, developing a JIACTF-like function[30] in OMB or elsewhere in the EOP, creating an entity similar to President Eisenhower's Operations Coordinating Board,[31] or establishing some other entity that, among other things, assists in assessing department and agency performance and oversees federal compliance with cybersecurity standards. Unless and until such an office is established, the work of the JIACTF should continue.[32]

---

[26] Electronic Frontier Foundation, Submission to White House Cyber Revew, at 1.
[27] Center for National Security Studies, Letter to National Security Council, April 8, 2009, at 2.
[28] TechAmerica, Response to 60-Day Cyber Security Review, at 6.
[29] Ari Schwartz and Gregory Nojeim (Center for Democracy and Technology), letter to National Security Council, March 20, 2009, at 4-5.
[30] JIACTF activities include reviewing target achievements, recent accomplishments, planned activities and schedules, risks and mitigation strategies, budget, staffing, performance measures, and critical issues as presented in department and agency quarterly report submissions.
[31] The board was established by Executive Order 10483 to provide for the integrated implementation for national security policies by several agencies. Some of its main functions included: assuring coordination and implementation of National Security policies, developing agreed upon plans of operations, and reporting to the NSC on actions taken. *See* Alfred Dick Sander, *Eisenhower's Executive Office*, Greenwood Press, Westport, 1999, at 128. *See also* Executive Order 10483, *Establishing the Operations Coordinating Board*, September 2, 1953.
[32] Congressional Research Service, Report for Congress, *The Executive Office of the President: An Historical Overview*, November 26, 2008, at 21.

Review Laws and Policies

The President's cybersecurity policy official should work with departments and agencies to recommend coherent unified policy guidance where necessary in order to clarify authorities, roles, and responsibilities for cybersecurity-related activities across the Federal government. Law applicable to information and communications networks is a complex patchwork of Constitutional, domestic, foreign, and international laws that shapes viable policy options. In the United States, this patchwork exists because, throughout the evolution of the information and communications infrastructure, the Federal government enacted laws and policies to govern aspects of what were very diverse industries and technologies.

As traditional telecommunications and Internet-type networks continue to converge and other infrastructure sectors adopt the Internet as a primary means of interconnectivity, law and policy should continue to seek an integrated approach that combines the benefits of flexibility and diversity of applications and services with the protection of civil liberties, privacy rights, public safety, and national and economic security interests. A paucity of judicial opinions in several areas poses both opportunities and risks that policy makers should appreciate—courts can intervene to shape the application of law, particularly in areas involving Constitutional rights. Policy decisions will necessarily be shaped and bounded by the legal framework in which they are made, and policy consideration may help identify gaps and challenges in current laws and inform necessary developments in the law. That process may prompt proposals for a new legislative framework to rationalize the patchwork of overlapping laws that apply to information, telecommunications, networks, and technologies, or the application of new interpretations of existing laws in ways to meet technological evolution and policy goals, consistent with U.S. Constitutional principles. However, pursuing either course risks outcomes that may make certain activities conducted by the Federal government to protect information and communications infrastructure more difficult.

The Administration should partner appropriately with Congress to ensure adequate law, policies, and resources are available to support the U.S. cybersecurity-related missions. Congress has demonstrated interest and bipartisan leadership regarding the cybersecurity-related needs of the Nation, and the Administration would benefit from Congressional knowledge and experience. The cybersecurity policy official, working with departments and agencies, should consult with industry to understand the impact of laws and policies on business operations.

Strengthen Federal Leadership and Accountability for Cybersecurity

Effective leadership anchored at the White House alone will not be sufficient to achieve the broad range of objectives necessary to lead the United States in the digital age. Leadership and accountability must extend throughout the Federal government. Including cybersecurity among the President's management priorities and assessing the progress of departments and agencies against stated goals would provide additional means to ensure accountability and progress. The cybersecurity policy official—in consultation with NSC, OMB, NEC, and OSTP—would define the milestones and success criteria and raise the visibility of cybersecurity within all agency budgets.

To bring transparency and effective management to the overall portfolio for cybersecurity, OMB should use its program assessment framework to ensure departments and agencies use performance-based budgeting in pursuing cybersecurity-related goals. A formal program assessment framework for cybersecurity would have departments and agencies define each program's purpose and goal as well as identify metrics to evaluate whether goals are achieved.[33] The CNCI has used a variation on this approach successfully.

Department and agency leaders must be held accountable, as required by the Federal Information Security Management Act (FISMA) of 2002. The Administration should work with Congress to update and strengthen this legislation. Performance plans of the department and agency leadership should include reporting on progress made to secure systems by each department and agency. The Federal government should develop options to hold department and agency leadership accountable for compliance with cybersecurity policies and to enforce implementation of appropriate cybersecurity procedures.

Elevate State, Local, and Tribal Leadership

State, local, and tribal governments should consider the need to elevate cybersecurity as an issue by designating a single leader to ensure effective coordination between Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and State Homeland Security Advisors (HSAs). The review team heard from representatives of the National Governors Association that cybersecurity is the weakest link in their efforts to protect critical infrastructure assets in their individual states.[34,35] HSAs can spend funds under a number of Department of Homeland Security (DHS) grant programs for cybersecurity efforts, but historically grant funds to a large extent have not been prioritized for cybersecurity. State, local, and tribal governments should consider whether to elevate cybersecurity as an issue and should ensure that CIOs, CISOs, and HSAs coordinate to achieve a robust defensive posture.

[33] *See* Institute for Information Infrastructure Protection, *National Cyber Security Research and Development Challenges Related to Economics, Physical Infrastructure, and Human Behavior: An Industry, Academic, and Government Perspective,* 2009, at 5, 29.
[34] Meeting with representatives of Multi-State Information Sharing and Analysis Center, March 6, 2009.
[35] Meeting with representatives of National Governors Association, March 25, 2009.

II. Building Capacity for a Digital Nation

The Nation is at a crossroads. Computers have transformed nearly every aspect of daily life, both at home and in the workplace. Online banking, shopping, and tax-filing are commonplace. The Nation's infrastructure is undergoing a revolution as digital and network technologies are being integrated across large systems with programs such as Smart Grid and the Next Generation Air Traffic System. Components of the recently enacted American Recovery and Reinvestment Act encourage the deployment of modern information and communications infrastructure to improve America's competitiveness and use technology to solve some of the Nation's most pressing problems. The United States faces the dual challenge of maintaining an environment that promotes innovation, open interconnectivity, economic prosperity, free trade, and freedom while also ensuring public safety, security, civil liberties, and privacy.

The general public needs to be well informed to use the technology safely. In addition, the United States needs a technologically advanced workforce to remain competitive in the 21st Century economy. In schools, math and science must be a priority. The United States should initiate a K-12 cybersecurity education program for digital safety, ethics, and security; expand university curricula; and set the conditions to create a competent workforce for the digital age. As the President has noted, "America faces few more urgent challenges than preparing our children to compete in a global economy."[36] To help achieve these goals, the Nation should:

- Promote cybersecurity risk awareness for all citizens;[37,38]
- Build an education system that will enhance understanding of cybersecurity and allow the United States to retain and expand upon its scientific, engineering, and market leadership in information technology;
- Expand and train the workforce to protect the Nation's competitive advantage; and
- Help organizations and individuals make smart choices as they manage risk.

Increase Public Awareness

Broad public awareness of the risks of online activities and how to manage them will require an effective communications strategy. The Federal government, in partnership with educators and industry, should conduct a national cybersecurity public awareness and education.[39] The President's cybersecurity policy official should lead the development and direct the implementation of this public awareness strategy and should seek endorsement by Congress; State, local, and tribal governments; the private sector; and the civil liberties and privacy communities. The strategy should

[36] www.whitehouse.gov/agenda/education, "Education," April 2, 2009, at 1.
[37] Cross-Sector Cyber Security Working Group (CSCSWG) Response to 60-day Cyber Review Questions, March 16, 2009, at 4.
[38] Business Executives for National Security, Cyber Strategic Inquiry 2008, December 2008, at 8.
[39] A 2008 study conducted by the organization Educational Technology Policy, Research, and Outreach, College of Education, University of Maryland concluded that education on cyber-ethics, cyber-safety, and cybersecurity is inadequate. Davina Pruitt-Mentle, Ph.D., 2008 National Cyberethics, Cybersafety, Cybersecurity Baseline Study, October 2008, Section 4, at 45, http://staysafeonline.mediaroom.com/index.php?s=67&item=44.

involve public education about the threat and how to enhance digital safety, ethics, and security. Malicious actors often take advantage of people's willingness to accept information from or provide personal information over the Internet. This campaign should focus on public messages to promote responsible use of the Internet and awareness of fraud, identity theft, cyber predators, and cyber ethics. Past successful public safety campaigns such as *Smokey Bear* on fire safety and the *Click It or Ticket* campaign for seat belt safety could be used as a model to inform and persuade the public about the importance of cybersecurity. These public service campaigns should focus on making cybersecurity popular for children and for older students choosing careers. Celebrities, the generation that has grown up with the technology, and new types of media can play critical roles in delivering the message effectively.

Increase Cybersecurity Education

Similar to the period after the launch of the Sputnik satellite in October, 1957, the United States is in a global race that depends on mathematics and science skills. According to a report published by *The Economist,* talented information technology (IT) employees "are already in short supply everywhere, but the situation will get tougher, as the nature of skills needed is changing. In addition to technical knowledge, tomorrow's IT employee will require expertise in project management, change management and business analysis." The study notes that the United States continues to boast the most positive environment for IT firms in the world, combining scale and quality in the key areas that promote competitiveness: education, infrastructure, encouragement of innovation, and legal protection.[40] The 2007-2008 Taulbee Survey on Computing Degree and Enrollment Trends, however, showed a continued decline in U.S. computer science and engineering bachelor's degree production to about half of its 2004 peak.[41] The Nation cannot afford to see this decline continue.[42]

The Federal government, with the participation of all departments and agencies, should expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy. Existing programs should be evaluated and possibly expanded, and other activities could serve as models for additional programs. For example:

- The National Science Foundation (NSF) in 2006 began to solicit grant proposals under its "Pathways to Revitalized Undergraduate Computing Education." This program seeks to develop a "U.S. workforce with the computing competencies and skills imperative to the Nation's health, security and prosperity in the 21st Century."[43]
- Scholarships have provided direct incentives for students to pursue not only cybersecurity education, but also careers in the Federal government. NSF and DHS sponsor the Scholarship for Service program in 34 institutions.[44] More than a thousand students received support

[40] The Economist Intelligence Unit, *The means to compete, Benchmarking IT industry competitiveness,* July 2007, at 3.
[41] Stuart Zweben, Computing Degree and Enrollment Trends, from the 2007-2008 CRA Taulbee Survey, 2008, at 4, www.cra.org/taulbee/CRATaulbeeReport-StudentEnrollment-07-08.pdf.
[42] *See also* Committee on Prospering in the Global Economy of the 21st Century, *Rising Above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future,* National Academies Press, 2007.
[43] www.nsf.gov/news/news_summ.jsp?cntn_id=109691.
[44] www.sfs.opm.gov, U.S. Office of Personnel Management, Federal Cyber Service: Scholarship for Service.

during the first eight years of the program, with more than 80 percent receiving jobs in the Federal government. The NSF stresses that the proven synergy between research and education cannot be over-emphasized in light of the pressing need to expand the workforce.[45]

- The National Centers of Academic Excellence in Information Assurance Education and Research, founded in 1988 by the National Security Agency and co-sponsored by DHS since 2004, promotes higher education in information assurance in 94 institutions in 38 States and the District of Columbia.[46] These centers have built partnerships beyond the most well-known institutions to include community, Hispanic, and historically Black colleges. The Defense Department also sponsors the Information Assurance Scholarship Program in those institutions.
- The National Collegiate Cyber Defense Competition, the Mathematical Association of America's Math Olympiad, the Department of Energy's Science Bowl, and the Siemens Foundation's Math, Science, and Technology Competition offer competition-oriented models. A group of academics organized by NSF cited DARPA's grand challenges, the Malcolm Baldrige National Quality Award, and the competition to create the Advanced Encryption Standard as other models.[47]

Expand Federal Information Technology Workforce

The President's cybersecurity policy official, in coordination with the ICI-IPC, should consider how to better attract cybersecurity expertise and to increase retention of employees with such expertise within the federal service. Departments and agencies have had success attracting new employees from industry, but the time required to obtain, transfer, or renew security clearances leads to lost opportunities. Federal employees need to be able to build portfolios and advance careers in ways they might not be able to do within a single agency. Shared training and rotational assignments across agencies and potentially with the private sector would not only be efficient, but would promote beneficial cross-fertilization and the building of professional networks.

Promote Cybersecurity as an Enterprise Leadership Responsibility

The Federal government should continue to facilitate programs and information sharing on threats, vulnerabilities, and effective practices across all levels of government and industry. It is not enough for the information technology workforce to understand the importance of cybersecurity; leaders at all levels of government and industry need to be able to make business and investment decisions based on knowledge of risks and potential impacts. State, local, and tribal governments face similar issues. State governments often serve as incubators for innovation and thus may be able to provide lessons learned in managing information and communications infrastructure. The Federal government should continue to work with industry to identify and disseminate effective practices in secure design and operation of information technology products.

[45] NSF, "Responses to Questions Posed by Ms. Melissa Hathaway during her Presentation at the National Science Foundation on March 18, 2009," March 31, 2009, at 1.
[46] www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml.
[47] *See* NSF, *supra* note 45.

III. Sharing Responsibility for Cybersecurity

The Federal government cannot succeed in the many facets of securing cyberspace if it works in isolation. The public and private sectors' interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure upon which businesses and government services depend. Government and industry leaders—both nationally and internationally—need to delineate roles and responsibilities, integrate capabilities, and take ownership of the problem to develop holistic solutions. Only through such partnerships will the United States be able to enhance cybersecurity and reap the full benefits of the digital revolution. The global challenge of securing cyberspace requires an increased effort in multilateral forums. This effort should seek—in continued collaboration with the private sector—to improve the security of interoperable networks through the development of global standards, expand the legal system's capacity to combat cyber crime, continue to develop and promote best practices, and maintain stable and effective Internet governance.

Improve Partnership Between Private Sector and Government

The Federal government has the responsibility to protect and defend the country, and all levels of government have the responsibility to ensure the safety and well-being of their citizens. The private sector, however, designs, builds, owns, and operates most of the network infrastructures that support government and private users alike. Industry and governments share the responsibility for the security and reliability of the infrastructure and the transactions that take place on it and should work closely together to address these interdependencies. There are various approaches the Federal government could take to address these challenges, some of which may require changes in law and policy.

Private-sector engagement is required to help address the limitations of law enforcement and national security. Current law permits the use of some tools to protect government but not private networks, and vice versa. Industry leaders can help by engaging in enterprise information sharing and account for the corporate risk and the bottom line impacts of data breaches, corporate espionage, and loss or degradation of services. Industry leaders can demand higher assurance from vendors and service providers while taking responsibility to create more secure software and equipment. Businesses need effective means to share detection methods, information about breaches and attack methods, remediation techniques, and forensic capabilities with each other and the Federal government.

If the risks and consequences can be assigned monetary value, organizations will have greater ability and incentive to address cybersecurity. In particular, the private sector often seeks a business case to justify the resource expenditures needed for integrating information and communications system security into corporate risk management and for engaging partnerships to mitigate collective risk. Government can assist by considering incentive-based legislative or regulatory tools to enhance

the value proposition and fostering an environment that facilitates and encourages partnership and information sharing.[48, 49, 50]

The President's cybersecurity policy official should work with relevant departments and agencies and the private sector to examine existing public-private partnership and information sharing mechanisms to identify or build upon the most effective models. Public-private partnerships have fostered information sharing and served as a foundation for U.S. critical infrastructure protection and cybersecurity policy for over a decade. During that time, the Federal government and the private sector have engaged in a number of forums on cybersecurity and information and communications infrastructure issues.[51]

These groups perform valuable work, but the diffusion of effort has left some participants frustrated with unclear delineation of roles and responsibilities, uneven capabilities across various groups, and a proliferation of plans and recommendations. As a result, government and private-sector personnel, time, and resources are spread across a host of bodies engaged in sometimes duplicative or inconsistent efforts. Partnerships must evolve to clearly define the nature of the relationship, the roles and responsibilities of various groups and their participants, the expectations of each party's contribution, and accountability mechanisms. The Federal government should streamline, align, and provide resources to existing organizations to optimize their capacity to identify priorities, enable more efficient execution, and develop response and recovery plans.

The 60-day review considered a number of models of effective public-private partnerships.[52] While these models perform very different functions, they share important attributes. Each has a clearly defined institutional mission, well-defined roles and responsibilities for participants, and a clear value proposition that creates incentives for members to participate. Each model also mitigates concerns that would otherwise discourage participation by establishing and maintaining an environment of trust among the members. Existing cybersecurity partnership bodies might apply the most effective characteristics of these models.

Evaluate Potential Barriers Impeding Evolution of Public-Private Partnership

Some members of the private sector continue to express concern that certain federal laws might impede full collaborative partnerships and operational information sharing between the private sector and government. For example, some in industry are concerned that the information sharing and collective planning that occurs among members of the same sector under existing partnership

[48] Written testimony of Scott Charney (Microsoft) to the House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, March 10, 2009, at 4-5.
[49] CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency,* December 2008, at 49ff.
[50] Internet Security Alliance, *Issue Area 3: Norms of Behavior—Hathaway Questions,* March 24, 2009, at 2, 4-7
[51] These include organizations such as the Critical Infrastructure Partnership Advisory Council (CIPAC) and its constituent bodies such as the Enduring Security Framework, the Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs); the Federal Bureau of Investigation's InfraGard; the U.S. Secret Service's Electronic Crimes Task Forces; the National Security Telecommunications Advisory Committee (NSTAC); the National Infrastructure Advisory Council (NIAC); the Homeland Security Advisory Council; and the associated subcommittees and working groups.
[52] These include the National Cyber-Forensics & Training Alliance, the Cross-Sector Cybersecurity Working Group (CSCSWG), and a consultancy model from the United Kingdom.

models might be viewed as "collusive" or contrary to laws forbidding restraints on trade.[53] Industry has also expressed reservations about disclosing to the Federal government sensitive or proprietary business information, such as vulnerabilities and data or network breaches. This concern has persisted notwithstanding the protections afforded by statutes such as the Trade Secrets Act and the Critical Infrastructure Information Act, which was enacted specifically to address industry concerns with respect to the Freedom of Information Act (FOIA). Beyond these issues, industry may still have concerns about reputational harm, liability, or regulatory consequences of sharing information. Conversely, the Federal government sometimes limits the information it will share with the private sector because of the legitimate need to protect sensitive intelligence sources and methods or the privacy rights of individuals.

These concerns do not exist in isolation. Antitrust laws provide important safeguards against unfair competition, and FOIA helps ensure transparency in government that is essential to maintain public confidence. The civil liberties and privacy community has expressed concern that extending protections would only serve as a legal shield against liability. In addition, the challenges of information sharing can be further complicated by the global nature of the information and communications marketplace. When members of industry operating in the United States are foreign-owned, mandatory information sharing, or exclusion of such companies from information sharing regimes, can present trade implications.

As part of the partnership, government should work creatively and collaboratively with the private sector to identify tailored solutions that take into account both the need to exchange information and protect public and private interests and take an integrated approach to national and economic security. These solutions should identify clear, actionable objectives for the sharing of data and define standards for incident reporting. The private sector would be more comfortable with sharing solutions that do not require data ownership changing hands, such as occurs with the British model of using vetted information security providers as a nexus for combining data rather than the government.

Finally, the Federal government should engage academia, civil liberties and privacy groups, advocates of open government, and consumers to ensure that government policy adequately considers the broad set of interests that they represent. Few problems can be reduced to a discrete question of process, policy, or technology. Changes in technology often precipitate policy considerations and may require changes in existing processes. Changes in policy (for example, adoption of regulation or tax incentives) can affect decisions regarding procurement or technological research and development. The Federal government could also consider ways in which it could focus more resources on research into possible "game-changing" areas, such as behavioral, policy, and incentive-based cybersecurity solutions. The interwoven nature of these issues underscores the need to ensure that all stakeholders' interests are represented.

[53] For example, the Sherman Antitrust Act, 15 U.S.C. §§ 1-7 (2004).

Partner Effectively With the International Community

International norms are critical to establishing a secure and thriving digital infrastructure. The United States needs to develop a strategy designed to shape the international environment and bring like-minded nations together on a host of issues, including acceptable norms regarding territorial jurisdiction, sovereign responsibility, and use of force. In addition, differing national and regional laws and practices—such as those laws concerning the investigation and prosecution of cybercrime;[54] data preservation, protection and privacy; and approaches for network defense and response to cyber attacks—present serious challenges to achieving a safe, secure, and resilient digital environment. Addressing these issues requires the United States to work with all countries—including those in the developing world who face these issues as they build their digital economies and infrastructures—plus international bodies, military allies, and intelligence partners.

In the past decade, federal communications, infrastructure, and cybersecurity-related policies developed along multiple paths. A more integrated approach to policy formulation would ensure mutually reinforcing objectives and allow the United States to leverage its international opportunities with consistent, more effective positions. The United States should adopt an integrated approach to national interests across a range of substantive areas—including cybersecurity and the protection of free speech and other civil liberties—to develop consistent policies.

The President's cybersecurity policy official should, working with departments and agencies, strengthen and integrate interagency processes to formulate and coordinate international cybersecurity-related positions. In addition, the Federal government—continuing the long-term history of collaboration with the private sector—should develop a proactive engagement plan for use with international standards bodies. This would include taking stock of current policies and coordinating the development, refinement, or reaffirmation of positions to ensure that the full range of cybersecurity-related economic, national security, public safety, and privacy interests are taken into account.[55] More than a dozen international organizations—including the United Nations, the Group of Eight, NATO, the Council of Europe, the Asia-Pacific Economic Cooperation forum, the Organization of American States, the Organization for Economic Cooperation and Development, the International Telecommunication Union (ITU), and the International Organization for Standardization (ISO)—address issues concerning the information and communications infrastructure.[56] New organizations are beginning to consider cybersecurity-related policies and activities, while others are expanding the scope of their existing work. These venues consider policies and conduct activities that sometimes conflict and often overlap. Agreements, standards, or practices promulgated in these organizations have global effects and cannot be ignored. The sheer number, variety, and differing focuses of these venues strain the capacity of many governments, including the United States, to engage adequately.

[54] For example, the Council of Europe Convention on Cybercrime is an important international effort to achieve consistency in cybercrime laws and law enforcement efforts. Although the United States and many developed countries are parties to this agreement, most countries are not signatories or have not ratified the treaty.
[55] CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency,* December, 2008, at 11-13.
[56] *Id.*

The President's cybersecurity policy official should work with departments and agencies to enhance the identification, tracking, and prioritization of international venues, negotiations, and discussions where cybersecurity-related agreements, standards, activities, and policies are being developed. Past experience indicates the United States will need to remain engaged in a range of international activities. The Federal government should then increase its work with the private sector and other countries to ensure full engagement in appropriate forums with respect to the issues that are most important to U.S. interests in the future of the global information and communications infrastructure. The United States and its international allies should leverage each other's participation in regional or other forums to drive common policy objectives, focus the work of existing international organizations, and limit duplication of effort among them. For example, standards for cybersecurity forensics are being developed in both the ITU and the ISO. The United States also should identify opportunities to promote the security and growth of the information and communications infrastructure in projects undertaken in forums devoted to broader topics.

Working with the private sector, the Federal government should coordinate and expand international partnerships to address the full range of cybersecurity-related activities, policies, and opportunities associated with the information and communications infrastructure upon which U.S. businesses, government services, the U.S. military, and nations depend. New agreements between governments and industry may need to be documented to enable international information sharing as well as strategic and operational collaboration. The Federal government should increase resources and attention dedicated to conducting outreach and building foreign capacity. For example, the United States should accelerate efforts to help other countries build legal frameworks and capacity to fight cybercrime and continue efforts to promote cybersecurity practices and standards. The United States also should work with allies to ensure the stability and global interoperability of the Internet, while increasing security and reliability for all users.[57]

[57] U.S. Chamber of Commerce, Letter to National Security Council, March 27, 2009, at 3.

IV. Creating Effective Information Sharing and Incident Response

The United States needs a comprehensive framework to facilitate coordinated responses by government, the private sector, and allies to a significant cyber incident. Federal, State, local, and tribal governments should work with industry to improve the plans and resources they have in place in advance to detect, prevent, and respond to significant cybersecurity incidents. Because such incidents are likely to affect interconnected networks across government and industry sectors, coordination of such plans and activities is important before, during, and after significant incidents. For example, despite advance warning and instructions on how networks could be protected, had the "Conficker" worm activated on April 1, 2009 with a malicious payload, some federal departments and agencies were not prepared to respond.

Build a Framework for Incident Response

During a significant cyber incident, as with other major national incidents, only the White House has the authority to coordinate the wide array of capabilities and authorities involved in incident response. Departments and agencies conduct their relevant mission responsibilities in line with overall White House strategic direction. The President's cybersecurity policy official should be the White House action officer for cyber incident response (a similar role to the action officers who help the White House monitor terrorist attacks or natural disasters).

The Federal government should have a clear and authoritative cyber incident response framework that needs to be documented in a revised Cyber Incident Annex for the National Response Framework. To date, federal responses to cyber incidents have not been unified. For situations involving National Security/Emergency Preparedness (NS/EP) communications, Executive Order 12472 delineates established authorities and processes; however, under current law and policy, each department and agency is responsible for deciding on and implementing measures to isolate, secure, and restore its own cyber networks and data.

Responsibility for a federal cyber incident response is dispersed across many federal departments and agencies because of the existing legal, but artificial, distinctions between national security and other federal networks. Depending on the character of an incident—for example, a major vulnerability, a criminal attack, or a military incident—different departments or agencies may have or share the lead role for response, while others may never learn of the event. Moreover, the lead for the overall incident may not be clear. Although each player has defined areas of expertise and legal authorities, they are difficult to pull together into a single coordinated structure. Any consolidation of authorities in a unified structure may require legislation. The ICI-IPC process should define roles, responsibilities, and resources for different departments and agencies with respect to incident response—harmonized or enhanced as necessary—recognizing the different aspects of incident response and the different strengths various communities—network security, law enforcement, intelligence, and military—bring to the table.

Numerous commentators have stressed the importance of developing thresholds for incident reporting and response. Network operators and service providers deal daily with large numbers of incidents that do not rise beyond the "nuisance" level. Hidden among these low-level incidents are a relatively few sophisticated, potentially high-impact intrusions or attacks that are difficult to detect. Knowledge of the technical details of such incidents would be of great interest to operators of other government and private-sector networks to help them defend their own networks against similar threats, as well as to law enforcement and intelligence entities tracking and seeking to stop criminal and foreign cybersecurity-related threat activities.

Network Operators and Service Providers

The Internet is operated by a combination of businesses that manage operations and provide services for their customers. Network operators build and maintain information and communications infrastructure in order to provide connectivity and bandwidth for customers. Service providers may provide an access gateway to the Internet, security services, storage or processing services, or access to information (for example, Internet addresses or news) and applications (for example, search engines). Individual companies may provide a unique mixture of access, information, and services (for example, social networks).

The Federal government—in collaboration with State, local, and tribal governments and industry—should develop a set of threat scenarios and metrics that all can use for risk management decisions, recovery planning, and prioritization of R&D. Modeling and simulation capabilities should be developed to help exercise these plans and determine potential levels of damage.

The ICI-IPC should develop clear, enforceable rules for timely reporting of incidents by departments and agencies to enable an effective and efficient interagency response. Departments and agencies are uneven in their incident reporting outside their own boundaries. The overall federal response would benefit from immediate reporting of significant events across a wider range of departments and agencies having incident response roles.

The President's cybersecurity policy official, working with the ICI-IPC, should determine the most efficient and effective method of developing and maintaining situational awareness and incident response capabilities. The CNCI effort should continue to improve federal network defenses but consider the need for adjustments or additions to implementation plans. In particular, the President's cybersecurity policy official should:

- Work with the private sector to explore how best to apply technical capabilities to the defense of the national infrastructure and what legal framework would be required to ensure the protection of privacy rights and civil liberties.
- Review the operational concept and the implementation of the National Cybersecurity Center (NCSC) to determine whether its proposed responsibilities, resource strategy, and governance are adequate to enable it to provide the shared situational awareness necessary to support cyber incident response efforts.
- Continue to pursue the goal of the Trusted Internet Connection program to reduce the number of government network connections to the Internet but reconsider goals and

timelines based on a realistic assessment of the challenges. Some departments and agencies during the past two years made progress reducing the number of connections and beginning the deployment of systems that will help the Federal government prevent as well as detect malicious behavior. The government, however, still has considerable work to do before full capability is achieved and may need to consider additional policies to enable full implementation of the strategy.

- Evaluate and continue, as appropriate—in ongoing consultation with the civil liberties and privacy community—pilot deployments of intrusion detection and prevention systems for the benefit of federal networks, evaluate the performance of these systems, and continue studies of the issues that would arise if such capabilities were used with State government systems. These sensors will be vital to gaining situational awareness for federal networks, and the government will benefit from any policy, legal, or technology lessons learned as these deployments move forward.
- Explore—in collaboration with industry and the civil liberties and privacy community—additional, long-term architectures for intrusion detection and prevention systems.

The Federal government should improve its ability to provide strategic warning of cyber intrusions and attacks to the President. The Federal government should continue to leverage the Nation's long-term investments in the fundamental development of cryptologic and information assurance technologies and the necessary supporting infrastructure. These investments, along with other intelligence capabilities, are critical to national strategic warning for attacks through cyberspace. In addition, the Federal government should identify any gaps in law enforcement capacity or investigative authority needed to defend the Nation's infrastructure. Any new authorities would need to be consistent with the protection of civil liberties and privacy rights.

The U.S. Government should invest in processes, technologies, and infrastructure that will help prevent cyber incidents. Options include increased security testing, investment in systems that automate or centralize network management, and more restricted connectivity to the Internet for some unclassified systems.

The government needs a reliable, consistent mechanism for bringing all appropriate information together to form a common operating picture. Federal cybersecurity centers often share their information, but no single entity combines all information available from these centers and other sources to provide a continuously updated, comprehensive picture of cyber threats and network status, to provide indications and warning of imminent incidents, and to support a coordinated incident response. The Defense Department is responsible for aggregating information on network health and status, attempted intrusions, and cyber attacks for its networks, the Intelligence Community for its networks, and US-CERT for civilian federal agencies and to some extent the private sector. Law enforcement and intelligence agencies collect information on criminal and foreign cyber-related threat activities but require additional capacity to deal with the scale of criminal activities.

The Federal government should consider whether available alternative or reserve communications would be adequate in the event of a major disruption of information and communications

infrastructure, particularly as information and communications networks converge. Replacement or repair of infrastructure may also require additional planning and resources, particularly in the event of physical damage to networks or hard-to-replace components of the power grid.

The Federal government should develop processes between all levels of government and the private sector to assist in preventing, detecting, and responding to cyber incidents by leveraging existing resources. To help build situational awareness related to the information and communications infrastructure, the Federal government should leverage existing resources such as the Multi-State Information Sharing and Analysis Center and the 58 State and local Fusion Centers that have been set up around the country.

Enhance Information Sharing To Improve Incident Response Capabilities

Information is key to preventing, detecting, and responding to cyber incidents. Network hardware and software providers, network operators, data owners, security service providers, and in some cases, law enforcement or intelligence organizations may each have information that can contribute to the detection and understanding of sophisticated intrusions or attacks. A full understanding and effective response may only be possible by bringing information from those various sources together for the benefit of all.

The Federal government should work with State, local, and tribal governments and the private sector—including data owners, network operators, and experts on privacy and civil liberties—to develop options for cybersecurity-related information sharing that address concerns with privacy and proprietary information and make information sharing mutually beneficial in the national interest. Private companies are concerned about the potential uses of their information. The government must protect privacy rights, law enforcement equities, intelligence sources and methods, and government information that would provide unfair competitive advantages. Clarity and accountability for both government and the private sector are needed to address these concerns. Possible options include:

- Creation of a not-for-profit non-governmental organization to serve as a trusted third-party host where government and private sector information may be shared to enhance the security of critical government and private-sector networks. Such an organization could leverage commercial services without disrupting the growing security service market.
- Continued engagement between the Federal government (e.g., law enforcement agencies) and individual firms or groups of firms—possibly with the participation of State, local, and tribal governments—that could achieve a level of voluntary information sharing within a particular sector or region beyond what could be achieved in a broader setting.

The Administration should consider, in consultation with affected parties and Congress, developing tailored incentives for information sharing. These measures might include, as a last resort, regulatory measures as part of an integrated approach to satisfying society's interests in robust and resilient critical infrastructures, civil liberties and privacy protections, and maintaining the fair and open economic markets that underlie the U.S. economic system. Privacy enhancing

technologies such as encryption or controlled access authentication could ameliorate some risks in sharing information.

The Federal government should undertake a comprehensive review of policies (such as security classification and clearance requirements) that inhibit interagency sharing of cybersecurity information, seek improvements in information sharing, and ensure that they preserve civil liberties and privacy rights and appropriate protection for sensitive information. Current policies governing the collection, use, retention, and dissemination of information by federal departments and agencies vary greatly based on statutory authorities, privacy and civil liberties concerns, sources and methods concerns, and historical practice. These policies present significant barriers to sharing cybersecurity information across the Federal government. This review should take into account the progress that the Federal government has made through the Security and Suitability Reform Initiative and the Information Sharing Environment effort in examining all facets of the security and suitability processing components.

The Federal government should work with the private sector to develop standards for incident reporting by private-sector network operators to the Federal government. Industry has expressed concerns about reporting cyber incidents to which they have fallen victim, including the potential for negative impacts from resulting shareholder concerns, market reactions, or regulatory action.[58] One industry group has proposed a government-industry working group to define sector-specific cyber incident thresholds that warrant reporting to security officials.[59] Use of such information by the government would require rules and oversight, particularly for the protection of privacy rights and civil liberties. Another way to increase reporting is through consideration of appropriate data breach notification laws that require notification to the public and to the government, including law enforcement entities that could pursue investigations. The Federal government also should examine the effectiveness and scope of existing reporting requirements for regulated markets.

At the same time, the Federal government needs to define processes and rules for sharing its incident reporting with the private sector. Formulation of these rules should consider classification and privacy issues. In addition, the Federal government should help the research community gain access, with appropriate controls, to cybersecurity-related event data that could be used to develop tools, test theories, and develop workable solutions. Such sharing would need to address the protection of sensitive or proprietary data and personal identity information.

The Federal government should explore expanded sharing of information about network incidents and vulnerabilities with major allies, seeking bilateral or multilateral arrangements that improve cybersecurity consistent with the protection of other U.S. economic and security interests and the protection of civil liberties and privacy rights. International collaboration makes effective government-private sector collaboration in the United States more challenging. Legitimate private-sector concerns over sharing information will increase if the government plans to share that information with other countries. Once again, clarity and accountability are needed for control, dissemination, and use of information shared by the private sector with the Federal government, including under-

[58] TechAmerica, Response to 60-Day Cyber Security Review, March 21, 2009.
[59] Cross-Sector Cybersecurity Working Group (CSCSWG), Response to 60-Day Cyber Review Questions, March 16, 2009, at 11-12.

standings governing the use of information shared between the United States and the international community.

Improve Cybersecurity Across All Infrastructures

The Federal government should work with the private sector to define public-private partnership roles and responsibilities for the defense of privately owned critical infrastructure and key resources. The common defense of privately-owned critical infrastructures from armed attack or from physical intrusion or sabotage by foreign military forces or international terrorists is a core responsibility of the Federal government. Similarly, government plays an important role in protecting these infrastructures from criminals or domestic terrorists. The question remains unresolved as to what extent protection of these same infrastructures from the same harms by the same actors should be a government responsibility if the attacks were carried out remotely via computer networks rather than by direct physical action. Most private network operators and service providers consider it to be their responsibility to maintain and defend their own networks, but key elements of the private sector have indicated a willingness to work toward a framework under which the government would pursue malicious actors and assist with information and technical support to enable private-sector operators to defend their own networks.[60]

The Federal government should consider options for incentivizing collective action and enhance competition in the development of cybersecurity solutions. For example, the legal concepts for "standard of care" to date do not exist for cyberspace. Possible incentives include adjustments to liability considerations (reduced liability in exchange for improved security or increased liability for the consequences of poor security), indemnification, tax incentives, and new regulatory requirements and compliance mechanisms.

The President's cybersecurity policy official should work with all levels of government, the private sector, and our international partners to develop strategies and plans to encourage the development of innovative cybersecurity solutions and ensure the security and resilience of infrastructure systems. Infrastructure examples include:

- The Administration should assist international financial institutions, such as the World Bank and the International Monetary Fund, with the necessary information, tools, and expertise and encourage their use of best practices to protect their information systems, which suffered a series of serious intrusions in 2008.[61]

[60] CSCSWG, Response to 60-Day Cyber Review Questions, March 16, 2009; TechAmerica input to 60-Day Cyber Review, March 21, 2009, at 1-2; NSTAC Response to 60-Day Cyber Group, March 12, 2009, at 3-4; Information Technology and Communications SCCs, Response to White House Cyber Review Questions, March 20, 2009.

[61] www.foxnews.com/story/0,2933,435681,00.html, *World Bank Under Cyber Siege in 'Unprecedented Crisis',* October 10, 2008; www.foxnews.com/story/0,2933,452348,00.html, *Cyber-Hackers Break into IMF Computer System,* November 14, 2008.

- The American Recovery and Reinvestment Act reserves funding to advance the use of health information technology. Protection of patient information will be critical to gaining public acceptance as electronic record keeping becomes more pervasive and accessible through the Internet.
- The Department of Energy should work with the Federal Energy Regulatory Commission to determine whether additional security mandates and procedures should be developed for energy-related industrial control systems. In addition, as the United States deploys new Smart Grid technology, the Federal government must ensure that security standards are developed and adopted to avoid creating unexpected opportunities for adversaries to penetrate these systems or conduct large-scale attacks.
- The Department of Transportation's Federal Aviation Administration (FAA) has developed a long-term plan for transitioning to the Next-Generation Air Traffic Control System while still maintaining the current system. The Department's Inspector General on March 18, 2009 advised the House Committee on Transportation and Infrastructure Subcommittee on Aviation of the need to assess potential security vulnerabilities and develop a robust cybersecurity strategy and design.[62]

[62] www.oig.dot.gov/item.jsp?id=2442, Department of Transportation, Statement of the Inspector General before the Committee on Transportation and Infrastructure Subcommittee on Aviation, House of Representatives, "Federal Aviation Administration: Actions Needed to Achieve Mid-Term NextGen Goals," March 18, 2009, at 7.

V. Encouraging Innovation

Resiliency Requirements

The infrastructure must be resilient against physical damage, unauthorized manipulation, and electronic assault. In addition to protection of the information itself, a risk mitigation strategy for cyberspace must focus on the devices used to access the infrastructure, the services provided by the infrastructure, supporting elements of the networks, and all means of moving, storing, and processing information. The strategy also must include prevention, mitigation, and response against threats to or subversion of the people who operate and benefit from the infrastructure, the processes that run or take advantage of the infrastructure, and the supply chains used to build and maintain the infrastructure.

The information and communications sector is moving toward a converged platform where data, voice and video applications share a common infrastructure. The decentralized nature of the current Internet model allows individuals and entrepreneurs to develop and deploy innovative applications at the edges of the network without obtaining permission. Innovation has sparked new multi-billion dollar businesses that have revolutionized the way users interact with the network and each other. As technology becomes more critical to the United States, maintaining confidence and trust in this constantly evolving infrastructure is essential. The President has called for the federal government to work with industry on the development of "next-generation secure computers and networking for national security applications," "tough new standards for cybersecurity and physical resilience," and "standards for securing personal data."[63]

The United States should harness the full benefits of innovation to address cybersecurity concerns. Many technical and network management solutions that would greatly enhance security already exist in the market place but are not always used because of cost or complexity. In addition, existing solutions can only do so much given the underlying design of the Internet architecture. In the long run, openness and innovation will help create a stronger infrastructure with transparency and accountability. Federal policy must address national security requirements, protection of intellectual property, and the availability and continuity of infrastructure, even when it is under attack by sophisticated adversaries. The Federal government also must be careful not to create policy and regulation that inhibits innovation or results in inefficiencies or less security.

The Future

According to a 2006 National Academies Report, *Renewing U.S. Telecommunications Research,* "Telecommunications networks are large, complex systems whose reliability, security, and evolvability are dependent on the development of a coherent and well-conceived architectural concept."[64] The report goes on to note that:

[63] www.whitehouse.gov/agenda/homeland_security/#protect-our-information-networks, The Agenda, Homeland Security, "Protect Our Information Networks."

[64] http://sites.nationalacademies.org/cstb/CompletedProjects/CSTB_042246, Robert Lucky and Jon Eisenberg, editors, Committee on Telecommunications Research and Development, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, National Research Council of the National Academies, "Renewing U.S. Telecommunications Research," 2006, at 36-37.

> "[M]ultiple vendors' products are used to configure U.S. telecommunications infrastructure and deliver services … that cross provider boundaries. As a result of the industry's shift to a horizontal structure and its fragmentation into a large number of firms, neither vendors nor service providers are prepared to take responsibility for end-to-end systems design."

As a result, no single, integrated vision exists to guide decision-making by the private sector, academia, and government about policies, standards, research, market development, or procurement. The Federal government, the private sector, and other stakeholders together should define technology-neutral performance and security objectives for future infrastructure, both to meet its own requirements as a consumer as well as in its capacity as a steward of the public interest. The Federal government and its partners should create a family of coordinated national information and communications infrastructure objectives, customized by sectors and organizations. These objectives could consider different models of computing platforms or network control concepts, and the emergence of technology solutions from government, academic, or industry research programs.

The movement of data and services to third-party network-based servers, referred to as the "cloud," introduces new policy challenges for the private sector and governments around the globe. The movement of data across jurisdictional boundaries presents challenges for law enforcement, the protection of privacy and civil liberties as defined by different countries, and liability decisions in the event of data or network breaches. Some customers will seek to limit where service providers move and store data, whereas others with multinational operations will seek to take advantage of geographic and time-zone diversity.

Infrastructure Security Visions

A number of efforts exist to define visions for some technology or infrastructure sectors. For example, the U.S. Department of Energy, in collaboration with industry, in 2005 published a 10-year roadmap for securing control systems used in the power grid (see *www.controlsystemsroadmap.net*). The vision for this effort is that by 2015 "control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber attack with no loss of critical function." An advisory group for the Defense Advanced Research Project Agency (DARPA) describes defense of current Internet Protocol-based networks as a losing proposition and calls for an "independent examination of alternate architectures," leading to experimentation and evaluation of the best candidates. According to a March 2009 briefing, DARPA is proceeding with a six-month analysis of alternatives.

Link R&D Frameworks to Infrastructure Development

Under the leadership of the President's cybersecurity policy official, in collaboration with other EOP entities and the ICI-IPC, the Federal government should provide a framework for research and development strategies that focus on game-changing technologies that will help meet infrastructure objectives, building on the existing Networking and Information Technology Research and Development (NITRD) strategies and other R&D-related work. The Federal government should

greatly expand coordination of these strategies with industry and academic research efforts to avoid duplication, leverage and synchronize complementary capabilities and agendas, and ensure that technology transitions and enters into the marketplace.

- To enhance U.S. competitiveness, the Federal government should work with industry to develop migration paths and incentives for the rapid adoption of research and technology development, including encouragement of collaboration between academic and industrial laboratories.
- The Federal government, in collaboration with the private sector and other stakeholders, also should use the infrastructure objectives and the R&D framework to help define goals for national and international standardsbodies.

Establish Identity Management as an Option

We cannot improve cybersecurity without improving authentication, and identity management is not just about authenticating people. Authentication mechanisms also can help ensure that online transactions only involve trustworthy data, hardware, and software for networks and devices. With the systems available today for most Internet transactions, the electronic equivalent of cues people use to establish trust might be absent, incomplete, or difficult to understand and act upon.[65] Identity management has the potential to help individuals and organizations form trusted communities based on varying degrees of identity exposure and mutually agreed accountability, while helping exclude unwanted intruders or inappropriate membership. Identity management also has the potential to enhance privacy through additional protection against the inappropriate release of personal identifiable information.

The Federal government—in collaboration with industry and the civil liberties and privacy communities—should build a cybersecurity-based identity management vision and strategy for the Nation that considers an array of approaches, including privacy-enhancing technologies. The Federal government must interact with citizens through myriad information, services, and benefit programs and thus has an interest in the protection of the public's private information as well. Increased use of on-line transactions involving financial, health, and commerce require a basis for building trust between the parties to a transaction.

- The Nation should implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy.
- The National Science and Technology Council's (NSTC's) Subcommittee on Biometrics and Identity Management in 2008 published a report that provides a vision for future federal identity management and a series of research and development recommendations.[66] The Federal government should use this report as a starting point for identity management strategies.

[65] See www.microsoft.com/mscorp/twc/endtoendtrust/vision.aspx, Scott Charney, "Establishing End to End Trust," Microsoft, 2008, at 5.
[66] www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf, Executive Office of the President, National Science and Technology Council, Identity Management Task Force Report, July 2008.

- The Federal government should work with international partners to develop policies that encourage the development of a global, trusted eco-system that protects privacy rights and civil liberties and governs appropriate use of law enforcement activities to protect citizens and infrastructures.

The Federal government, following the guidance of Homeland Security Presidential Directive 12 (HSPD-12), is seeking to leverage the federal interoperable identity credentialing mechanism across the federal enterprise. The Federal government should ensure resources are available for full federal implementation of HSPD-12. The Federal government also should consider extending the availability of federal identity management systems to operators of critical infrastructure and to private-sector emergency response and repair service providers for use during national emergencies.

Integrate Globalization Policy with Supply Chain Security

One of the results of the information technology revolution and free trade policies is a global environment for research, design, manufacturing, and servicing of information and communications products by corporations with facilities spread across the globe. This global marketplace has created tremendous benefits for U.S. industry by opening markets worldwide for high-tech U.S. goods and services. However, the emergence of new centers for manufacturing, design, and research across the globe raises concerns about the potential for easier subversion of computers and networks through subtle hardware or software manipulations. Counterfeit products have created the most visible supply problems, but few documented examples exist of unambiguous, deliberate subversions.

A broad, holistic approach to risk management is required rather than a wholesale condemnation of foreign products and services. The challenge with supply chain attacks is that a sophisticated adversary might narrowly focus on particular systems and make manipulation virtually impossible to discover. Foreign manufacturing does present easier opportunities for nation-state adversaries to subvert products; however, the same goals could be achieved through the recruitment of key insiders or other espionage activities.

The best defense may be to ensure U.S. market leadership through continued innovation that enhances U.S. market leadership and the application of best practices in maintaining diverse, resilient supply chains and infrastructures. The President's cybersecurity policy official, working with departments and agencies, should:

- Define procurement strategies through the General Services Administration, building on work by the National Security Agency for the Department of Defense, for commercial products and services in order to create market incentives for security to be part of hardware and software product designs, new security technologies, and secure managed services;
- Expand partnerships with State, local, and tribal governments and international partners to maximize the market influence of these procurements;
- Work with Congress to identify mechanisms that would enable departments and agencies—under appropriate, limited situations—to incorporate threat information into acquisition decisions; and

- Work with industry to provide threat information and identify best practices for managing supply chain and insider risks, both from economic and threat perspectives.

Maintain National Security/Emergency Preparedness (NS/EP) Capabilities

The Federal government's obligation to protect the American people and to provide for the common defense includes a responsibility to ensure that the Nation can communicate and respond in times of crisis. The communications system itself might bear the brunt of such events and must have resilience or the capability to recover to manage a response and preserve governmental functions. The Communications Act of 1934 authorized the President, if he deems it necessary in the national security or defense and the requisite threshold condition exists, to use, control, or close communications services, systems, and networks under the jurisdiction of the Federal Communications Commission in conditions ranging from "state of public peril" to "war." Executive Order 12472 established a joint government-industry National Coordinating Center to assist in the initiation, coordination, restoration and reconstitution of communications services or facilities under all conditions of crisis or emergency. NSPD-51/HSPD-20 on "National Continuity Policy" (May 4, 2007) assigns roles in the Federal government regarding continuity communications.

The Department of Homeland Security (DHS) is working toward the goal of providing national security and emergency users with access to the converged information services of next-generation networks in a manner that provides a high likelihood of service success during disasters and other events that cause public users to experience severe degradation or loss of communications services. The national security enhancements to next-generation networks will include services for data, voice, and video. The DHS effort is complicated by the variations in architectures envisioned by the major carriers and service providers. As such, DHS is examining and comparing different approaches and will seek industry consensus on approaches to be brought forward for consideration by standards organizations. The Federal government should:

- Develop a coordinated plan for national security and emergency preparedness communications capabilities over next-generation networks, including milestones and funding requirements;
- Develop options for additional services the Federal government could acquire or direct investments the government could make in the information and communications infrastructure to enhance the survivability of communications during a time of natural disaster, crisis, or conflict;
- Coordinate with international partners and standards bodies to support next-generation NS/EP communications capabilities in a globally distributed next-generation environment;[67] and
- Ensure that efforts associated with the development of Executive Branch continuity communications architectures and next-generation services programs are adequately staffed and resourced.

[67] Also recommended by "NSTAC Response to the Sixty Day Cyber Study Group," March 12, 2009, at 18, 21.

VI. Action Plans

The review team recommends the near-term and mid-term actions listed in Tables 2 and 3.

TABLE 2: NEAR-TERM ACTION PLAN
1. Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.
2. Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.
3. Designate cybersecurity as one of the President's key management priorities and establish performance metrics.
4. Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
5. Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government.
6. Initiate a national public awareness and education campaign to promote cybersecurity.
7. Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.
8. Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement
9. In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.
10. Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

TABLE 3: MID-TERM ACTION PLAN
1. Improve the process for resolution of interagency disagreements regarding interpretations of law and application of policy and authorities for cyber operations.
2. Use the OMB program assessment framework to ensure departments and agencies use performance-based budgeting in pursuing cybersecurity goals.
3. Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy.
4. Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government.
5. Determine the most efficient and effective mechanism to obtain strategic warning, maintain situational awareness, and inform incident response capabilities.
6. Develop a set of threat scenarios and metrics that can be used for risk management decisions, recovery planning, and prioritization of R&D.
7. Develop a process between the government and the private sector to assist in preventing, detecting, and responding to cyber incidents.
8. Develop mechanisms for cybersecurity-related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial.
9. Develop solutions for emergency communications capabilities during a time of natural disaster, crisis, or conflict while ensuring network neutrality.
10. Expand sharing of information about network incidents and vulnerabilities with key allies and seek bilateral and multilateral arrangements that will improve economic and security interests while protecting civil liberties and privacy rights.
11. Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations.
12. Use the infrastructure objectives and the research and development framework to define goals for national and international standards bodies.
13. Implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy.
14. Refine government procurement strategies and improve the market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services.

Appendix A: Bibliography

Accenture, *"Secure Enterprise Network Consortium: Helping Provide Comprehensive Cyber Security Approaches for High Performance"* (undated)

Aliant, *"Developing a Telecommunications Roadmap: Preparing for the promise of convergence"* (undated)

American Chemistry Council, ChemITC, *"Making Strides to Improve Cyber Security in the Chemical Sector,"* 2009 Update, March 2009

American Chemistry Council, Christine Adams, untitled memorandum of the Chemical Sector Cyber Security Program's responses to four questions from the White House 60-day Cyber Policy Review (undated)

Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, and Securities and Exchange Commission, *"Interagency Paper on Sound Practices To Strengthen the Resilience of the U.S. Financial System,"* Federal Register, Volume 68, Number 70, April 18, 2003

Brecht, Lyle A., Capital Markets Research, *"National Cyber Systems Infrastructure Security Review Concept Paper,"* February 15, 2009

Business Executives for National Security, *"Commercial/Civil Cyber Community Snapshot"* (undated)

Business Executives for National Security, *"Cyber Strategic Inquiry: Enabling Change Through a Strategic Simulation and Megacommunity Concept",* December 2008

Business Executives for National Security, *"Cybersecurity Roundtable, March 19, 2009, City Club, Washington DC,"* March 26, 2009

Business Executives for National Security, *"National Cybersecurity Center Policy Capture"* (undated)

Business Software Alliance, *"National Security & Homeland Security Councils Review of National Cyber Security Policy,"* March 19, 2009

Carnegie Mellon CyLab, Pradeep Khosla, *"Information Security for the Next Century: Why we need an information-centric approach to data protection"* (undated)

Carnegie Mellon University, Lynn Robert Carter, *"Computing Infrastructure Risk: Issue, Analysis, and Recommendation,"* December 23, 2008

Center for Applied Cybersecurity Research, Indiana University, Fred H. Cate, *"Comments to the White House 60-Day Cybersecurity Review,"* March 27, 2009

Center for Democracy and Technology, *"Comprehensive Privacy and Security: Critical for Health Information Technology,"* Version 1.0, May 2008

Center for Democracy and Technology, letter from Ari Schwartz and Gregory T. Nojeim, March 20, 2009

Center for Education and Research in Information Assurance and Security, Purdue University, presentation by Eugene Spafford entitled *"NITRD Strategic Plan Forum,"* February 2009

Center for Infrastructure Protection, George Mason University, *"The CIP Report,"* Volume 7, Number 8, February 2009

Center for National Security Studies, letter from Kate Martin, April 4, 2009

Center for Progressive Regulation, Rena Steinzor, *"Democracies Die Behind Closed Doors: The Homeland Security Act and Corporate Accountability,"* March 12, 2003

Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency, *"Securing Cyberspace for the 44th Presidency,"* December 2008

Center for the Development of Technological Leadership, University of Minnesota, presentation by S. Massoud Amin entitled *"Smart Grid: Opportunities and Challenges Toward a Stronger and Smarter Grid"* at the 2009 MIT Energy Conference – Accelerating Change in Global Energy, Cambridge, Massachusetts, March 6, 2009

Computer Science & Artificial Intelligence Laboratory, Massachusetts Institute of Technology, presentation by John C. Mallery entitled "*Mobilizing for Cyber Defense: Transforming Computation & Networking*," March 2009

Computing Research Association, paper by Stuart Zweben entitled *"Computing Degree and Enrollment Trends: From the 2007-2008 CRA Taulbee Survey"* (undated)

Congressional Research Service, report by Harold C. Relyea entitled *"The Executive Office of the President: An Historical Overview,"* updated November 26, 2008

Congressional Research Service, report by John Rollins and Anna C. Henning entitled *"Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations,"* March 10, 2009

Davidson, Mary Ann, Oracle Corporation, *"The Monroe Doctrine in Cyberspace",* March 2009

Defense Advanced Research Projects Agency, *"The National Cyber Range: A National Testbed for Critical Security Research"* (undated)

Department of Defense, *"Defense Security Information Exchange (DSIE) A partnership for the Defense Industrial Base"* (undated)

Department of Defense, Lt. Col. Michael Barry and Steven D. Shirley, *"DoD Cyber Crime Center (DC3) Prioritization,"* March 12, 2009

Department of Health & Human Services, Office of the National Coordinator for Health Information technology, *"The ONC-Coordinated Federal Health IT Strategic Plan: 2008-2012,"* June 3, 2008

Department of the Treasury, *"2008 Update to Banking and Finance Sector-Specific Plan: Sector Profile and Goals"* (undated)

Department of the Treasury, *"2008 Update to Banking and Finance Sector-Specific Plan: Appendix B: Statutory Authorities"* (undated)

Department of the Treasury, FSSCC/FBIIC Cyber Security Intelligence and Information Sharing Work Groups, *"Roadmap for Improved Information Sharing: Situational Analysis and Recommendations for Action"* (undated)

Department of the Treasury, memorandum regarding 60-day cyber review questions (undated)

Economist Intelligence Unit, The, *"The means to compete: Benchmarking IT Industry Competitiveness",* July 2007

Educational Technology, Policy, Research, and Outreach, *"2008 National Cyberethics, Cybersafety, Cybersecurity Baseline Study",* study conducted on behalf of the National Cyber Security Alliance, October 2008

Electronic Frontier Foundation, letter from Lee Tien and Peter Eckersley (undated)

Financial Services Information Sharing and Analysis Center, letter from William B. Nelson, March 23, 2009

Forrester, *"IT Security Remains An Integral Part Of The Enterprise: The State Of Enterprise IT Security: 2008 To 2009",* January 29, 2009

Gourley, Bob, Crucial Point LLC, *"Cloud Computing and Cyber Defense,"* March 21, 2009

Gourley, Bob, Crucial Point LLC, *"Open Source Software and Cyber Defense,"* March 30, 2009

Harper, Jim, Cato Institute, *"Government-Run Cyber Security? No, Thanks,"* TechKnowledge Newsletter, Issue #123, March 13, 2009

Harris Interactive, *"Online Security and Privacy Study",* conducted on behalf of Microsoft and the National Cyber Security Alliance, March 2009

Information Sciences Institute, University of California, *"Report on National Cyber Defense Initiative Industry Workshop: Report and Recommendations,"* March 27, 2009

Information Systems Audit and Control Association, *"IS Standards, Guidelines and Procedures for Auditing and Control Professionals,"* January 15, 2009

Information Technology Information Sharing and Analysis Center, letter from Brian Willis, February 27, 2009

Information Technology Sector Coordinating Council and Communications Sector Coordinating Council, *"Response to White House Cyber Review Questions,"* March 20, 2009

Intelligence and National Security Alliance, *"60 Day Cyber Study INSA Response,"* March 26, 2009

Intelligence and National Security Alliance, *"Critical Issues for Cyber Assurance Policy Reform: An Industry Assessment,"* March 26, 2009

Intelligence and National Security Alliance, *"The Missing Link in U.S. Cybersecurity,"* March 21, 2009

Internet Corporation for Assigned Names and Numbers, *"Factsheet: Root server attack on 6 February 2007,"* March 1, 2007

Internet Security Alliance, *"ISA Comments to Hathaway on creating an International Cyber Security Anchor Program"* (undated)

Internet Security Alliance, *"ISA Initial Comments on Hathaway 60-Day review – a top 10 list of Cyber Principles"* (undated)

Internet Security Alliance, *"The Cyber Security Social Contract Policy Recommendations for the Obama Administration and 111th Congress: A Twenty-First Century Model for Protecting and Defending Critical Technology Systems and Information"* (undated)

Internet Security Alliance, *"The Economic and Security Costs of Obsolescent Computer Laws"* March 24, 2009

Internet Security Alliance, paper by Jeff Brown, Raytheon Company, entitled *"A National Model for Cyber Protection Through Disrupting Attacker Command and Control Channels,"* March 2009

Internet Security Alliance, paper by Larry Clinton entitled *"Cross cutting Issue #2 How Can we create public private partnerships that extend to action plans that work?"* (undated)

Internet Security Alliance, paper by Larry Clinton entitled *"Cyber-Insurance Metrics and Impact on Cyber-Security"* (undated)

Internet Security Alliance, paper by Larry Clinton entitled *"Issue Area 3: Norms of Behavior—Hathaway Questions"* (undated)

Internet Security Alliance, paper by Scott Borg entitled *"Securing the Supply Chain for Electronic Equipment: A Strategy and Framework"* (undated)

Internet Security Alliance, paper by Sentar, Inc., *"Position paper for Obama 60 Day review on Cyber Security: Utilization of Small Business (SBs) for Innovative Cyber Security Research and Development",* March 26, 2009

Jackson, William, *"Agency Award'Federal Aviation Administration: Protect and serve,"* Government Computer News, October 7, 2007

Kellermann, Tom, Core Security Technologies, *"Proactive Public Policy per Cybersecurity,"* March 18, 2009

Kellermann, Tom, Core Security Technologies, *"Red teaming idea in detail,"* March 11, 2009

Khater, Rami and Rachel Schaffer, Georgetown University, untitled memorandum, April 13, 2009

Markle Foundation, *"Nation at Risk: Policy Makers Need Better Information to Protect the Country,"* March 10, 2009

Massachusetts Institute of Technology, The Microphotonics Center, executive overview of the 2005 communications technology roadmap entitled *"Microphotonics: Hardware for the Information Age,"* 2005

National Association of State Chief Information Officers, NASCIO State CIO-CISO Cybersecurity Priorities Survey Summary, March 3, 2009

National Coordination Office for Networking and Information Technology Research and Development, Sally E. Howe, presentation entitled *"Workshop Deliverables: Roadmap, Hard Problems, and Report"* at the HCSS-Sponsored National Workshop on Beyond SCADA: Networked Embedded Control for Cyber Physical Systems, November 8, 2008

National Cyber Forensics & Training Alliance and Cyber Initiative & Resource Fusion Unit, *"Cyber Fusion Center, Pittsburgh, PA: Executive Briefing"* (undated)

National Cyber Security Alliance and Symantec, *"NCSA-Symantec National Cyber Security Awareness Study: Newsworthy Analysis,"* October 2008

National Cyber Security Alliance, *"National Cyber Security Alliance in Brief"* (undated)

National Research Council, report edited by Robert W. Lucky and Jon Eisenberg entitled *"Renewing U.S. Telecommunications Research,"* 2006

National Science and Technology Council, Subcommittee on Biometrics and Identity Management, *"Identity Management Task Force Report 2008,"* 2008

National Science Foundation / Intelligence Advanced Research Projects Activity / National Security Agency, workshop report by David Evans, (University of Virginia) Principal Investigator, for the NSF/IARPA/NSA Workshop on the Science of Security, Berkeley, California, November 17-18, 2008 (unpublished)

National Science Foundation, *"Notes for White House 60-day Cyber-Policy Review,"* March 25, 2009

National Science Foundation, *"NSF Security Program Overview,"* March 26, 2009

National Science Foundation, *"Responses to Questions Posed by Ms. Melissa Hathaway During Her Presentation at the National Science Foundation on March 18, 2009,"* March 31, 2009

National Security Telecommunications Advisory Committee, *"NSTAC Response to the Sixty-Day Cyber Study Group,"* March 12, 2009

Networking and Information Technology Research and Development Program, High Confidence Software and Systems Coordinating Group, *"High-Confidence Medical Devices: Cyber-Physical Systems for 21st Century Health Care,"* February 2009

Office of the Director of National Intelligence, Joint Interagency Cyber Task Force, Steven R.Chabinsky, presentation entitled *"Intrusion Detection and Prevention (What, Where, How and Who)"* (undated)

Pederson, Perry, Wurldtech Labs, *"Project Aurora and the Smart Grid"* (undated)

Pinkney, Kevin R., *"Putting Blame Where Blame is Due: Software Manufacturer and Customer Liability for Security-related Software Failure,"* Albany Law Journal of Science & Technology, Volume 13, 2002

Raduege, Harry D., Jr., *"Evolving Cybersecurity Faces a New Dawn,"* SIGNAL Magazine, December 2008

Raduege, Harry D., Jr., *"Future Defense Department Cybersecurity Builds on the Past,"* SIGNAL Magazine, February 08

SANS Institute, *"The United States Cyber Challenge,"* May 8, 2009

SAS Institute, *"INSA Cyber Task Force Submission"* (undated)

Schneider, Fred B., and Birman, Kenneth P., Cornell University, *"The Monoculture Risk put into Context,"* IEEE Security & Privacy, January/February 2009

Spafford, Eugene H. and Annie I Antón, *"The Balance of Privacy and Security,"* Controversies in Science and Technology, Vol II, ed. by Daniel Lee Kleinman, Karen A. Cloud-Hansen, Christina Matta, and Jo Handelsman, pub. MaryAnn Liebert, Inc, NYC, NY, 2008

Spoonamore, Stephen and Ronald L. Krutz, *"Smart Grid and Cyber Challenges: National Security Risks and Concerns of Smart Grid",* March 2009

SRI International, Computer Science Laboratory, technical report addendum by Phillip Porras, Hassen Saidi, and Vinod Yegneswaran entitled "Conficker C Analysis," March 19, 2009

TechAmerica, *"TechAmerica Response to 60-Day Cyber Security Review,"* March 2009

Trevithick, Paul, William Coleman, John Clippinger, and Kim Taipale, *"Identity and Resilience"* (undated)

U.S. Chamber of Commerce, letter from Ann Beauchesne, March 27, 2009

United States Congress, American Recovery and Reinvesment Act of 2009, Public Law 111-5

United States Congress, Year 2000 Information and Readiness Disclosure Act, Public Law 105-271

United States Government Accountability Office, David A. Powner, *"Information Technology: Federal Laws, Regulations, and Mandatory Standards for Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors,"* September 16, 2008

United States House of Representatives, 111th Congress, *"A bill to authorize the Secretary of Homeland Security to establish a program to award grants to institutions of higher education for the establishment or expansion of cybersecurity professional development programs, and for other purposes."* (H.R.266), as introduced in the House, January 7, 2009

United States House of Representatives, hearing before the Armed Services Committee, Subcommittee on Strategic Forces, *"Status of US Strategic Programs,"* March 17, 2009

United States House of Representatives, hearing before the Armed Services Committee, Subcommittee on Strategic Forces, *"Statement of General Kevin P. Chilton, Commander, United States Strategic Command,"* March 17, 2009

United States House of Representatives, hearing before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, *"Statement of Chairman Bennie G. Thompson, 'Reviewing the Federal Cybersecurity Mission,'"* March 10, 2009

United States House of Representatives, hearing before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, *"Testimony of Amit Yoran, Netwitness Corporation, 'Reviewing the Federal Cybersecurity Mission,'"* March 10, 2009

United States House of Representatives, hearing before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, *"Federal Cybersecurity Mission,"* March 10, 2009

United States House of Representatives, hearing before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, *"Statement for the Record of Seán P. McGurk, Director, Control Systems Security Program, National Cyber Security Division, National Protection and Programs Directorate, Department of Homeland Security,"* March 24, 2009

United States House of Representatives, hearing before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, Science and Technology, *"Statement of Chairwoman Yvette D. Clarke,"* March 10, 2009

United States House of Representatives, hearing before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, *"Statement of David Powner, Director, Information Technology Management Issues, United States Government Accountability Office, 'National Cybersecurity Strategy: Key Improvements are Needed to Strengthen the Nation's Posture,'"* March 10, 2009

United States House of representatives, hearing before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, *"Statement of James A. Lewis, Center for Strategic and International Studies, 'Reviewing the Federal Cybersecurity Mission,'"* March 10, 2009

United States House of Representatives, hearing before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, *"Testimony of Mary Ann Davidson, Chief Security Officer, Oracle Corporation,"* March 10, 2009

United States House of Representatives, hearing before the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, Science and Technology, *"Written Testimony of Scott Charney, Corporate Vice President, Microsoft Corporation's Trustworthy Computing, 'Securing America's Cyber Future: Simplify, Organize and Act,'"* March 10, 2009

United States House of Representatives, hearing before the Committee on Science and Technology, *"Statement of Dr. Christopher L. Greer, Director, National Coordination Office for Networking and Information Technology Research and Development,"* April 1, 2009

United States House of Representatives, hearing before the Committee on Transportation and Infrastructure, Subcommittee on Aviation, *"Statement of James C. May, President and CEO, Air Transport Association of America, Inc., 'Air Traffic Control Modernization and NextGen: Near-Term Achievable Goals,'"* March 18, 2009

United States House of Representatives, hearing before the Committee on Transportation and Infrastructure, Subcommittee on Aviation, *"Statement of The Honorable Calvin L. Scovel III, Inspector General, U.S. Department of Transportation, 'Federal Aviation Administration: Actions Needed to Achieve Mid-term NextGen Goals,'"* March 18, 2009

United States House of Representatives, hearing before the Permanent Select Committee on Intelligence, *"Annual Threat Assessment"* by Dennis C. Blair, Director of National Intelligence, February 25, 2009

United States House of Representatives, Permanent Select Committee on Intelligence, *"HPSCI White Paper on Cyber security,"* December 10, 2008

United States Secret Service, memorandum entitled *"Electronic Crime task Forces (ECTF)"* (undated)

United States Senate, 111th Congress, Senate Bill S.773, *"Cybersecurity Act of 2009",* as introduced in the Senate, April 1, 2009

United States Senate, 111th Congress, Senate Bill S.778, "*A bill to establish, within the Executive Office of the President, the Office of the National Cybersecurity Advisor",* as introduced in the Senate, April 1, 2009

United States Senate, hearing before the Committee on Energy and Natural Resources, *"Questions for Patrick Gallagher, National Institute of Standards and Technology,"* March 3, 2009

United States Senate, hearing before the Committee on Energy and Natural Resources, *"Statement of Patricia Hoffman, Acting Assistant Secretary for Electricity Delivery and Energy Reliability, U.S. Department of Energy,"* March 3, 2009

United States Senate, hearing before the Committee on Energy and Natural Resources *"Testimony of Patrick D. Gallagher, Ph.D., Deputy Director, National Institute of Standards and Technology, United States Department of Commerce,"* March 3, 2009

Vijayan, Jaikumar, *"PCI security standard gets flayed at House hearing,"* Computerworld, April 1, 2009

Appendix B: Methodology

The globally interconnected information and communications infrastructure often known as "cyberspace" underpins every facet of American society and provides critical support for the national economy, civil infrastructure, security, and military power. Recognizing its importance to the nation, the President directed the National and Homeland Security Councils to conduct a 60-day comprehensive, "clean-slate" review to assess U.S. cyberspace policies and structures. The review begins to carry out the President's pledge to "lead an effort, working with private industry, the research community and our citizens, to build a trustworthy and accountable cyber infrastructure that is resilient, protects America's competitive advantage, and advances our national and homeland security."

Defining the scope of the review and establishing a clear end-state goal

Pursuant to the President's direction, the White House staff established the review's scope and defined the end-state goal, which was vetted through the Interagency Policy Committee (IPC) process and approved by the NSC-HSC Deputies Committee. When achieved, that end goal of trusted and resilient communications and information infrastructures built through a national public-private partnership and action plan will:

- Enhance economic prosperity and facilitate U.S. market leadership in the information and communications industry;
- Enable the United States to deter, prevent, detect, defend against, respond to, and remediate interruptions and damage to U.S. information and communications infrastructure;
- Ensure U.S. capabilities to operate in cyberspace in support of national goals; while at the same time
- Protect privacy rights and preserving civil liberties.

This review addresses all missions and activities associated with the information and communications infrastructure, including computer network defense, military, and intelligence missions and the intersection thereof with information assurance, counter intelligence, counter terrorism and telecommunications policies. It seeks to identify the policy gaps, organizational redundancies, overlapping missions, legal questions, civil liberties and privacy concerns, and other unresolved issues across the above mission spaces. The review does not provide an in-depth analysis of options or an extensive audit of programs; rather, it presents the need for a more balanced and integrated policy-making approach to address the convergence of the Nation's economic and security interests in the digitally-dependent global environment of the 21st Century.

Inventorying requirements of cyber, communications, and homeland security and counter-terrorism mission areas as well as recommendations from government advisory boards and private-sector studies

During the first ten days, the review team inventoried more than 250 requirements (some overlapping) from the relevant Presidential policy directives, executive orders, national strategies, and studies from government advisory boards and private sector entities. The review team solicited input from departments and agencies on their specific cyber activities, authorities, and capabilities across these requirements and requested departments and agencies to identify any new or existing requirements that may not have been identified as part of the initial inventory. During this phase, governmental legal experts identified more than 80 issues associated with the scope of the 60-day cyber review. Those lawyers are addressing the highest priority legal issues in papers that identify common facts, applicable law, differences in legal interpretation, and options for resolution. In addition, the review team consulted governmental civil liberties and privacy officials to identify and assess relevant issues.

Capturing the viewpoints of key cyber stakeholders on requirements to meet the end-state goal

The review team reached out to a wide array of stakeholders inside and outside the Federal government. Recognizing that there are opportunities for everyone—academia, industry, and government—to work together to build a trusted and resilient communications and information infrastructure, the review team ensured that these stakeholders were aware of the review's scope and asked for input on pertinent areas of interest.

The engagement process included over 40 meetings and yielded over 100 papers that named specific recommendations and desired goals. Stakeholders' responses and public statements (e.g., Congressional testimony) helped to identify key requirements, illuminate policy gaps, suggest areas of improvement or collaboration, and frame the decision space for cyberspace policy. The review team synthesized the results into overarching themes and issues for further consideration.

In some cases, the individuals who submitted materials did so in their personal capacity as experts, rather than as representatives or affiliates of particular entities (such as universities). In all cases, the participants' submission of information does not imply that they endorse the results of the review in part or in full.

The Private Sector

The U.S. depends upon a privately owned, globally operated digital infrastructure. The review team engaged with industry to continue building the foundation of a trusted partnership. This engagement underscored the importance of developing value propositions that are understood by both government and industry partners. It also made clear that increasing information sharing is not enough; the government must foster an environment for collaboration. The following industry groups and venues participated: the Armed Forces Communications and Electronics Association

(AFCEA), Business Executives for National Security (BENS), the Business Software Alliance (BSA), the Center for Strategic and International Studies' (CSIS) Commission on Cybersecurity for the 44th Presidency, the Communications Sector Coordinating Council (C-SCC), the Cross-Sector Cyber Security Working Group (CSCSWG), the Defense Industrial Base Executive Committee, the Financial and Banking Information Infrastructure Committee (FBIIC), the Financial Services Sector Coordinating Council (FS-SCC), the Intelligence and National Security Alliance (INSA), the Internet Security Alliance (ISA), the Information Technology Sector Coordinating Council (IT-SCC), the National Infrastructure Advisory Council (NIAC), the National Security Telecommunications Advisory Committee (NSTAC), TechAmerica, and the U.S. Chamber of Commerce.

Civil Liberties and Privacy Community

Robust protections for civil liberties and privacy needed to be considered at the outset. The 60-day review team began a dialogue with key members of the civil liberties and privacy community, including both advocates and independent experts, to discuss measures for protecting the information and communications infrastructure and how those measures may impact individual users. The review team's civil liberties and privacy community engagement included affiliates of the American Civil Liberties Union, the American Library Association, the Cato Institute, the Center for Democracy and Technology, Carnegie Mellon University, Consumer Action, the Center on National Security Studies, Cornell University, the Electronic Frontier Foundation, the Electronic Privacy Information Center, George Washington University, Harvard University, Indiana University, Johns Hopkins University, OMB Watch, Ohio State University, the National Security Archive, and the University of California-San Diego.

Academic and Research Community

The academic and open cybersecurity research community has contributed many important technological innovations and continues to be a valuable resource for the future of the nation's efforts to design, build and deploy trustworthy systems. The National Science Foundation assembled more than sixty academics from universities across the country to contribute to the 60-day cyber policy review. Their areas of interest included privacy; computer networking and security; cryptography and web security; trust and risk; Internet commerce, usability, and feasibility; usable privacy and security; network security and architecture; theory of network security; biologically-inspired security; systems security; systems and software engineering; systems and wireless security and botnets; host security and usability; e-vote security; the power grid; clean-slate security; and theoretical computer science and nanotechnology, among other disciplines. These academics were affiliated with the following institutions: Brown University, Carnegie Mellon University, Columbia University, Cornell University, Dartmouth College, Georgia Tech, Indiana University, Johns Hopkins University, the Massachusetts Institute of Technology, New York University, North Carolina State University, Purdue University, Princeton University, SRI International, Stanford University, the University of California-Berkeley, the University of California-Santa Barbara, the University of Illinois at Urbana-Champaign, the University of New Mexico, the University of Southern California, the University of Washington, and Yale University.

State and Local Constituents

State governments are experiencing many of the same network intrusions and infections as the Federal government. Recognizing that the Nation must identify ways to leverage State resources, provide assistance, and continue cooperation, the 60-day cyber policy review team engaged with state Chief Information Security Officers (CISO) and Chief Information Officers (CIO) through the Office of Management and Budget's E-Government and Information Technology Office and the Department of Homeland Security's US-CERT. The Multi-State Information Sharing Advisory Council (MS-ISAC) and National Governors Association were also engaged to gain a better understanding of State and local needs.

Independent U.S. Government Agencies

While it is often preferable to allow markets to create appropriate incentives for desired behaviors, there are occasions when government intervention is necessary. Ensuring the health, security, and growth potential of the U.S. information and communications infrastructure will require a successful partnership between government and the private sector. The 60-day cyber policy review team reached out to regulatory agencies for their views on sound regulation for an effective marketplace. The Commodity Futures Trading Commission, the Federal Communications Commission, the Federal Energy Regulatory Commission, the Federal Reserve Board of Governors, the Federal Trade Commission, the Office of the Comptroller of the Currency (a component of the Department of the Treasury rather than an independent agency), and the Securities and Exchange Commission all provided information or met with the review team.

The 60-day cyber review team also met with independent agencies such as the Social Security Administration which uses on-line services to interact daily with the American public. Additional information was considered regarding the Federal Aviation Administration and the informational services it provides to the Nation.

The United States Congress

The 60-day cyber policy review team recognizes that Congress must be engaged at every stage of the review and will have important roles to play going forward. Creating and maintaining a transparent and connected democracy is a key tenet of the Administration. Accordingly, the review team engaged Members and staff of the Congress across 10 committees in both chambers and also provided a briefing to the House Cyber Caucus.

Foreign Partners

The United States cannot succeed by acting in isolation, because cyberspace crosses geographic and jurisdictional boundaries. The United States must work actively with countries around the world to make the digital infrastructure a trusted, safe, and secure place that enables prosperity for all nations. The 60-day cyber policy review team engaged with key U.S. allies to learn how they are organizing for this challenge and to understand their mission requirements and priorities. One area needing further study is whether and in what ways elements of the information and communications infrastructure ought to be treated as a global commons.

Conducting gap analyses, reviewing program effectiveness, and identifying policy gaps, overlaps, and opportunities for collaboration

The review team queried and analyzed responses from 21 Federal departments and agencies to identify areas where cyberspace policy gaps exist, where mission areas overlap, and where there are opportunities for collaboration between agencies. This analysis suggested that any complete national cyber policy must consider, at a minimum, the following elements:

- ***Governance:*** Encompasses U.S. Government (USG) structures for policy development and coordination of operational activities related to the cyber mission across the Executive Branch. This element includes reviewing overlapping missions and responsibilities that are the result of authority being vested with various departments and agencies.
- ***Architecture:*** Addresses the performance, cost, and security characteristics of existing information and communications systems and infrastructures as well as strategic planning for the optimal system characteristics that will be needed in the future. This element includes standards, identity management, authentication and attribution, software assurance, research and development, procurement, and supply chain risk management.
- ***Norms of Behavior:*** Addresses those elements of law, regulation, and international treaties and undertakings, as well as consensus-based measures, such as best practices, that collectively circumscribe and define standards of conduct in cyberspace.
- ***Capacity Building:*** Encompasses the overall scale of resources, activities, and capabilities required to become a more cyber-competent nation. These include resource requirements, research and development, public education and awareness, and international partnerships, and all other activities that allow the USG to interface with its citizenry and workforce to build the digital information and communications infrastructure of the future.

The review team also identified areas that cut across all of the foundational elements and included these in the analysis framework: Information Sharing and Access; Public-Private Partnerships; Legal, Policy, and Authorities; Protecting Civil Liberties and Privacy Rights; International Partnerships and Forums; Incident Response, and Research and Development.

Developing a roadmap to identify short-, mid-, and long-term issues, an organizational structure to address these issues, and an accountability mechanism to ensure compliance

The review team synthesized the input from the requirements compilation and the extensive engagement functions to begin developing a roadmap that outlines a way forward.

Within the roadmap, the team prioritized issues for further consideration. The roadmap includes an organizational structure and proposals for accountability mechanisms that will ensure coordinated policies.

This review produced recommendations on an optimal White House organizational construct to coordinate all issues related to U.S. and global information and communications infrastructures and capabilities. It also led to the broad outlines of a proposed interagency cyber policy action plan.

Appendix C: Growth of Modern Communications Technology in the United States and Development of Supporting Legal and Regulatory Frameworks

This paper highlights some of the significant historical milestones in the growth and convergence of modern communications media and information technology in the United States over the last century, along with the increasing importance of these media to support commercial, societal, and governmental purposes. It also attempts to trace at a high level some of the corresponding milestones in law, regulation, and policy that were intended to accommodate needs associated with these changing uses. Rooted in the Nation's experience with wire and radio media and communications in the 20th Century, present U.S. laws and policies governing cyberspace reflect serial attempts to keep pace with newly emerging challenges presented by the rapid technological and marketplace changes in communications, computing, networking, and security technologies.

This review is not meant to be exhaustive; nor does it seek to present legal analysis of the laws and instruments discussed.[1] Rather, it attempts only to capture noteworthy highlights of the historical progression to survey the landscape of Federal authorities that now apply to information and communications technology and systems. The picture that emerges shows this landscape to be an elaborate patchwork of domestic and international laws and structures that shape policy options.

Early Development and Use of the Media for Civil and Commercial Purposes

The development of the electric telegraph in the 1840s and the telephone in the late 1870s made rapid long-distance communications possible. Both media began in local areas and then rapidly spread to connect large parts of the Nation and the world. Fewer than five years after its introduction, over 47,000 telephones were being used in the United States. The growth of these communications media accelerated the pace of social interaction, migration, commerce, and government activities.

The telegraph and, to a greater degree, the telephone continued to be the principal media for telecommunications for most of the 20th Century. The introduction of undersea cables in the late 1850s enabled worldwide communications structures and the expansion of the leading telecommunications companies to a dominant position in the industry.

[1] The contents of this appendix do NOT constitute legal analysis, guidance or advice and may not be relied upon by any Federal officer, agency or department. The legal analysis in this appendix has not undergone an interagency clearance process and does not represent an official position of the United States government or any department or agency thereof. A working group of governmental legal experts supporting the 60-day cyber review is examining the function of, and relationship among, some of the various legal authorities noted herein. From among more than 80 issues submitted to the cyber review group, the lawyers group is reviewing the highest priority legal issues in papers that identify common facts, applicable law, and differences in legal interpretation.

The invention of "wireless telegraphy" (now known as "radio") at the turn of the 20th Century greatly increased the mobility of official and personal communications and made greater volumes of communications possible. Radio quickly emerged as both a medium for point-to-point (e.g., ship-to-shore) and point-to-multipoint telecommunications (e.g., police dispatch) and a mass medium for information, entertainment, and commerce. Fueled by technological advances like the amplifying vacuum tube in 1913, both coast-to-coast telephony and transatlantic radio transmission became possible, weaving the world even closer together. The utility and consequent worldwide adoption and rapid evolution of these new communications media prompted the creation of new legal and regulatory regimes both internationally and domestically to set rates, standardize terms of service, and allocate frequency bands to radio services by country.

The advent of international communications via telegraph led to the International Telegraph Union Convention and the formation of the International Telegraph Union in 1865, and the United States became a member in 1908. The Department of State has led U.S. delegations to this organization (and its successor) since the United States first joined it. Communication via radiotelegraph led to the International Radiotelegraph Convention in 1906.

On the domestic front, the Radio Act of 1912 established a radio licensing regime within the Department of Commerce and required certain ships to carry radios for communications. Due to conflict between amateur radio operators and the U.S. Navy and corporations, the Radio Act further regulated private radio communications, thus setting the precedent for federal regulation of wireless communications.

In the Radio Act of 1927, Congress directed the transfer of this radio frequency licensing regime from the Department of Commerce (with the notable exception of federal agencies' authorization to use radio frequencies) to a newly created five-member independent agency, the Federal Radio Commission. The Radio Act of 1927 also outlawed the interception of private radio messages and divulging their contents. Regulation of wireline communications remained separate from wireless, however, with responsibility shared between the Commerce Department and the Interstate Commerce Commission. Following on the popularity of radio, television debuted in the 1920s and by the 1950s was firmly entrenched.

The next noteworthy developments came less than a decade later, in 1934. First, the International Telegraph Convention and the International Radiotelegraph Convention combined, and the International Telegraph Union was renamed the International Telecommunication Union (ITU). In 1949, the ITU became a specialized agency of the United Nations. The ITU Constitution and Convention are updated every four years and will next be negotiated again in 2010 at the ITU Plenipotentiary Conference in Veracruz, Mexico.

Second, coinciding with the establishment of the ITU, Congress enacted the Communications Act of 1934, which replaced the Federal Radio Commission with a new agency, the Federal Communications Commission (FCC) and consolidated in it authorities for both wireless and wireline communications. In particular, the Communications Act gave the FCC broad authority to regulate:

> interstate and foreign commerce in communication by wire and radio so as to make available, without discrimination on the basis of race, color, religion, national origin, or sex, a rapid efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of the national defense, for the purpose of promoting safety of life and property through the use of wire and radio communication . . . .[2]

Since its inception, the FCC has remained the primary institution responsible for formulating and implementing U.S. policies and regulations governing private, commercial electronic communications within the United States and between the United States and other countries. Its jurisdiction over "communication by wire and radio" has been reinforced by multiple amendments to the Communications Act over the years. This has enabled the FCC to affect the economic and technical development of virtually all types of electronic communications, including telegraph, telephone service, cable television, radio, television, wireless telecommunications and, more recently, emerging advanced telecommunications technologies and services. Separate from the FCC, however, the White House with support from the Department of Commerce retained a role in management of the Federal government's use of radio spectrum, and in the development of executive branch policies related to communications, for another 44 years.[3]

Innovation in electronic communications continued to progress during the 1940s. The need to deliver television signals to communities in remote mountain areas led to the early development of community antenna television (CATV) systems, which, with the adoption of coaxial cable, and more recently fiber optic cable, would later evolve into the modern cable television systems that now compete with telephone companies to deliver video, voice, and data services to customers. It was also during this decade that radio and telephony intersected with the invention of the transistor and the advent of mobile radiotelephone technology. Broader commercial and public use of mobile telephone service began in the 1970s, and the first commercial cellular networks were developed in 1982 and 1983. By 2004, wireless subscribership in the United States had exceeded 180 million.

The first experimental communications satellite was launched in 1962. It was the first satellite to receive, amplify, and simultaneously re-transmit signals from earth. The development of satellite communications available not only to governments but also the commercial sector and individuals led to even greater volumes of communications worldwide.

As noted above, for most of the 20th Century, the White House directly managed executive branch communications policy and the Federal government's use of the radio spectrum, supported by the Department of Commerce. In 1978, however, the Carter Administration disaggregated and reorganized telecommunications functions within the Executive Branch. In Executive Order 12046,[4] President Carter dissolved the White House Office of Telecommunications Policy (OTP) and trans-

[2] 47 U.S.C. § 151.
[3] Over the course of time, telecommunications policy in the White House was managed variously by a Telecommunications Advisor to the President, 1951-53; the Office of Defense Mobilization (later the Office of Defense and Civilian Mobilization), 1953-61; the Office of Emergency Planning (later the Office of Emergency Preparedness), 1961-70; and, finally, the Office of Telecommunications Policy, 1970-78. *See* National Archives & Records Administration, *Records of the National Telecommunications and Information Administration,* § 417.1 Administrative History, available at http://www.archives.gov/research/guide-fed-records/groups/417.html?template=print.
[4] E.O. 12046, *Relating to the transfer of telecommunications functions* (March 27, 1978), 43 FR 13349, 3 C.F.R., 1978 Comp., p. 158.

ferred its responsibilities, respectively, either to the Commerce Department or back to the President for re-delegation to other components within his Executive Office.

Responsibility for Federal radio spectrum management and development and presentation of telecommunications and information policies on behalf of the Executive Branch were transferred to the Commerce Department, and a new agency, the National Telecommunications and Information Administration (NTIA), was established to perform them.[5] These responsibilities were codified by the NTIA Organization Act in 1992.[6] By contrast, OTP's responsibility to advise the President, and develop and establish policies, regarding procurement and management of Federal telecommunications systems, were reassigned to the Office of Management and Budget (OMB).[7] Similarly, OTP's responsibilities relating to emergency and national security communications were reassigned to the National Security Council (NSC) and the Office of Science and Technology Policy (OSTP).[8]

Use of Communications Technologies in Support of Critical Government Functions

As public adoption of each new generation of communications and information technology grew, use by government correspondingly increased. State, local, and tribal authorities have adopted these technologies for a variety of applications ranging from more efficient execution of routine administrative functions and improving government services and access to government information, to support for law enforcement efforts. The Federal government has employed evolving communications and information technologies for all of these purposes as well, but it has also applied them for critical national functions including *foreign affairs, military command and control,* and *intelligence* efforts.

For example, following the deployment of the first successful transatlantic cable in 1866, the telegraph became an important tool for U.S. diplomacy and remained so through most of the 20th Century. Spurred by the development of Morse Code, the telegraph was widely employed for military purposes as well during the U.S. Civil War, and as early as 1904, the U.S. Navy was using wireless telegraphy for communications with its bases in the Caribbean Sea.

Recognizing the pivotal importance of communications to support the execution of government functions during a crisis, Congress, by joint resolution in 1918, authorized the President to assume control of any telegraph, telephone, marine cable or radio system or systems in the U.S. and to operate them as needed for the duration of World War I.[9] Relying on this Congressional authorization, President Wilson issued a proclamation asserting possession, control and supervision over

[5] While NTIA is the principal adviser to the President on matters related to telecommunications, other Federal agencies routinely represent executive branch views on matters related to the public safety and national security before the FCC. For example, in the context of the Communications Assistance for Law Enforcement Act (CALEA), the Department of Justice and the Federal Bureau of Investigation have submitted comments regarding published industry standards that do not satisfy CALEA's requirements or adequately address law enforcement and national security equities.
[6] 47 U.S.C. § 901 *et seq.*
[7] E.O. 12046, *supra* note 4, § 3-1.
[8] Id. § 4. These responsibilities included the President's war power functions under Section 706 of the Communications Act, 47 U.S.C. § 606, policy direction of the development and operation of the National Communications System (NCS), and coordinating the development of policy, plans, programs and standards for the mobilization and use of the Nation's telecommunications resources during a crisis. *Id.* §§ 4-101, 4-201, 4-301.
[9] Pub. Res. No. 38, 40 Stat. 904.

every telegraph and telephone system within the United States.[10] To preserve support for critical government communications needs during times of crisis, Congress later included in Section 706 of the Communications Act of 1934 authority for the President to control private communications systems within the United States during wartime.[11]

As governments around the world increased their use of electronic communications for diplomatic, military, and other functions, vulnerabilities of long-range radio communications made it possible to intercept foreign communications from faraway locations without the knowledge of the communicators. The potential for "signals intelligence" (SIGINT) greatly increased. Conversely, the potential for interception of electronic communications led to the need for improved communications security (COMSEC) technologies and efforts: Nations including the United States sought more sophisticated means to protect their communications from interception, generally relying on electromechanical machines to encipher and decipher messages. COMSEC and Computer Security (COMPUSEC) practices were merged in the late 1980s to create Information Systems Security and, later, Information Assurance. Pursuant to Executive Order 12333, as amended, the Secretary of Defense serves as the Executive Agent for SIGINT and the Director of the National Security Agency (NSA) serves as Functional Manager for SIGINT and National Manager for National Security Systems.[12]

Use of electronic surveillance for legitimate purposes such as intelligence and law enforcement investigation, as well as for illegitimate purposes, spurred enactment of a number of laws intended to comprehensively address such activities. Congress enacted the first federal wiretap statute as a temporary measure to prevent disclosure of domestic telephone or telegraph communications during the First World War.[13] The Communications Act of 1934 extended the ban on intercepting and divulging of messages to telephone and telegraph communications. In 1968, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act (the Federal Wiretap Act),[14] and 18 years later enacted the Electronic Communications Privacy Act of 1986 (ECPA),[15] which substantially revised Title III to provide coverage for the technological advances developed in the area of electronic communications since the passage of the original act. In 1978, Congress enacted the Foreign Intelligence Surveillance Act (FISA),[16] which established the framework for conducting electronic surveillance for foreign intelligence purposes.[17]

World events and changes in the communications marketplace also prompted changes in government organizational structures and policies. In response to communications problems experienced during the Cuban Missile Crisis, President Kennedy in 1963 established the National Communications

[10] 40 Stat. 1807-1808.
[11] 47 U.S.C. § 606; *see also* 47 U.S.C. § 305 (Presidential authority over all U.S. government stations).
[12] E.O. 12333, *United States Intelligence Activities* (December 4, 1981), as amended by E.O. 13284 (2003), E.O. 13355 (2004), and E.O. 13470 (2008). E.O. 12333 encompasses much more than the discrete issues noted here; as amended, it provides the governance framework for all United States intelligence activities.
[13] Pub. L. No. 230, 65th Cong., 2d Sess., 40 Stat. 1017-18 (1918), 56 Cong. Rec. 10761-765.
[14] 18 U.S.C. § 2510 *et seq.*
[15] Pub. L. No. 99-508.
[16] 50 U.S.C. § 1801 *et seq.*
[17] While Title III governs domestic surveillance and FISA relates to surveillance conducted for foreign intelligence purposes, the two laws share several common characteristics. Both prescribe authorization procedures that must be followed before electronic surveillance can be conducted, including judicial approval of surveillance applications; minimization of interceptions by surveilling officials; and limitations on the use of intercepted information. Both statutes also impose criminal and civil penalties on unauthorized surveillance activities. *See* U.S. Department of Justice, *Criminal Resource Manual,* 1073 The Foreign Intelligence Surveillance Act, *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/title9/crm01073.htm.

System (NCS).[18] Two decades later, responding in part to the break-up of AT&T, President Reagan re-chartered and strengthened the NCS, increasing its membership and establishing an administrative structure to ensure that national telecommunications infrastructure is responsive to national security and emergency preparedness (NS/EP) needs.[19] By its terms, the executive order was intended to support "improved execution of national security and emergency preparedness telecommunications functions," but it did not address information systems, or converged information and communications networks which now provide the foundation for most critical NS/EP communications requirements.

Executive Order 12472 continued the disaggregation and realignment of telecommunications responsibilities started in E.O. 12046, especially with respect to NS/EP functions. First, it established two new roles, Executive Agent and Manager of the NCS, who were responsible for oversight and day-to-day administration of the NCS organization.[20] It also bifurcated responsibilities for certain NS/EP functions among elements within the Executive Office of the President (EOP). For example, it charged the NSC to provide policy direction for the exercise of the President's war power functions under the Communications Act but gave the OSTP responsibility to direct the exercise of those functions.[21] The E.O. created a similar split of responsibilities with respect to the exercise of the President's non-wartime emergency telecommunications functions; the identification, allocation, and use of the Nation's telecommunications resources during a crisis or emergency; and planning and oversight activities.[22]

Emergence of Computing, the Internet, and the Convergence of Information and Communications Technology

Computers. The development of electronic computing systems following World War II fostered the transition from analog to digital technology. Increasing miniaturization led to high adaptability of computers for many different modes of communications. The first e-mail program was created in 1971, and the first PC modem was invented in 1977, enabling digital computers to communicate with one another over analog telephone lines. The first popular computers for the mass consumer market first emerged in the early 1980s, coincident in time with the emergence of the Internet as a global network-of-networks. This new, retail computing capability was quickly adopted by government, private commercial entities, and the general public.

As the data speeds of modems progressively increased, computer users were encouraged to connect to the telephone network to access newly-emerging online services (e.g., CompuServe and America Online), which, in turn, fueled the market for new online applications and services of value to consumers. The World Wide Web, first conceptualized in 1984, came into widespread public use a decade later as a ubiquitous environment accessible through the telephone network. The corre-

[18] Presidential Memorandum of August 21, 1963.
[19] E.O. 12472, *Assignment of national security and emergency preparedness telecommunications functions* (April 3, 1984), 49 FR 13471. In particular, it established an interagency committee comprised of those 24 federal departments and agencies that own or lease telecommunications assets identified as part of the NCS or which bear policy, regulatory, or enforcement responsibilities of importance to NS/EP.
[20] The Executive Agent function was originally assigned to the Secretary of Defense, but was later reassigned to the Secretary of Homeland Security upon the creation of that Department following the terrorist attacks of September 11, 2001. *See* 6 U.S.C. § 121(g)(2); *see also* E.O. 13286, *Amendment of Executive Orders, and Other Actions, In Connection With the Transfer of Certain Functions to the Secretary of Homeland Security* (February 28, 2003) § 46.
[21] E.O. 12472, *supra* note 19, § 2(a)
[22] *Id.* §§ 2(b), (c).

sponding progressive migration from the traditional copper telephone infrastructure and co-axial cable to fiber optic infrastructure has delivered increased bandwidth and speed to users.

As information technology and systems evolved, Congress enacted a separate body of law governing computers and information systems. The Brooks Act,[23] enacted in 1965, gave the National Bureau of Standards—now the Department of Commerce's National Institute of Standards and Technology (NIST)—responsibilities for developing automatic data processing standards and guidelines pertaining to Federal computer systems. The responsibilities assigned to NBS, however, did not apply to the procurement of automatic data processing equipment or services by the Central Intelligence Agency or to what are now called "national security systems" by the Department of Defense. The Computer Security Act of 1987,[24] which further amended the Brooks Act, gave NIST the authority for developing standards and guidelines for the security of non-national security systems and required NIST to collaborate with NSA.

The Federal Information Security Management Act of 2002 (FISMA)[25] amended the Computer Security Act, leaving intact the roles of NIST and NSA, but it gave OMB expanded information security oversight responsibilities over all Executive Branch departments and agencies; it authorized the Director of OMB to require agencies to follow the standards and guidelines developed by NIST, review agency security programs annually and approve or disapprove them, and take authorized actions to ensure compliance. FISMA did not change, however, the dichotomy that exists in the treatment of civilian and national security systems.

While national security systems continued to be excluded from NIST oversight,[26] other regimes were established to deal with them, most notably National Security Directive 42. NSD-42, issued in July 1990, expanded the scope of a previously chartered national security telecommunications policy coordinating body to encompass information systems as well. In addition, it established a new body, the National Security Telecommunications and Information Systems Security Committee (NSTISSC). The NSTISSC was charged, among other things, to provide systems security guidance for national security systems for Executive Branch departments and agencies and to develop appropriate "operating policies, procedures, guidelines, instructions, standards, objectives, and priorities as may be required . . . ."[27] The NSTISSC shared many of the structural characteristics of the NCS, including an interagency membership structure (which included the Manager of the NCS) administered by an Executive Agent, which function was assigned to the Secretary of Defense, and a National Manager (the Director of NSA) that assists the Secretary in executing assigned information assurance responsibilities.[28]

---

[23] Public Law 89-306, *as amended by* the Paperwork Reduction Reauthorization Act of 1986, Public Laws 99-500 and 99-591.
[24] Public Law 100-235.
[25] Homeland Security Act of 2002, Pub. L. 107-296; *see also* Title III, e-Gov Act of 2002, Pub. L. 107-347.
[26] 15 U.S.C. § 278g-3, which incorporates the definition of NSS contained in 44 U.S.C. § 3542(b)(2). NSS are defined as "any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which — (A) involves intelligence activities; (B) involves cryptologic activities related to national security; (C) involves command and control of military forces; (D) involves equipment that is an integral part of a weapon or weapons system; or (E) is critical to the direct fulfillment of military or intelligence missions provided that this definition does not apply to a system that is used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications)."
[27] National Security Directive 42, National Policy for the Security of National Security Telecommunications and Information Systems (July 5, 1990), § 5(b). The NSTISSC has since been renamed the Committee on National Security Systems (CNSS). E.O. 13231, *Critical Infrastructure Protection in the Information Age* (October 16, 2001).
[28] *Id.* §§ 5, 6, 7. In particular, NSA may provide technical assistance to owners of national security systems as well as conduct vulnerability assessments to those systems and disseminate information on threats to and vulnerabilities of national security systems.

Development of the Internet. Consistent with the need to ensure the continuity of communications for these critical national security needs, the Federal government, in 1962, commissioned a study on how the government could maintain command and control over its missiles and bombers after a nuclear attack. This effort yielded a concept for a network that would break up the information into "packets" sent through various computers and could be reassembled at the destination location. Unlike the conventional hub and spoke telephone system available at the time, an attack on any one part of the proposed system would allow the undamaged portions to continue operating. During the 1960s, what is now the Department of Defense (DOD) Advanced Research Projects Agency (DARPA) sought to develop this network idea, eventually establishing ARPANET, a computer link between the University of California, Los Angeles, and the Stanford Research Institute, in 1969.[29]

ARPANET expanded significantly during the 1980s, interconnecting with numerous educational institutions and a growing number of companies that were participating in government research projects or providing services to entities participating in such projects. Moreover, during this time, other packet-switched networks were emerging in the United States and elsewhere around the world (e.g., Europe, Australia, Japan, Singapore, and Thailand) and seeking to connect to this "Internet."[30] This network-of-networks continued to grow over the course of the next decade until, in 1997, the United States government undertook to privatize the Internet's domain name and addressing system (DNS) in a manner intended to increase competition and facilitate international participation in its management.

A Shift in the Law, and the Emergence of "Cybersecurity"

As the Internet grew, the government, like the private sector, rapidly adopted this new medium for a wide variety of applications including interconnecting the civilian department and agency, defense, and intelligence community networks across the government to facilitate more rapid communications and common processing tasks. While this evolution was progressing, policy makers in Congress and the Executive Branch were separately considering dramatic changes to the legal and regulatory framework that had governed communications technologies and markets for decades. Invigorated by the emergence of competition in the long distance telephone market following the breakup of AT&T, policy makers reexamined regulatory frameworks that had historically perpetuated monopolistic market structures (e.g., local exchange telephone and cable television services) and sought to replace them with new regimes that would stimulate the emergence of competition, lowering costs for consumers and accelerating the development and deployment of advanced telecommunications infrastructures.

[29] Following on this research, international packet switching network standards were developed in collaboration with entities in other countries under the auspices of the ITU. During the 1970s, DARPA pursued further work on a network protocol that would permit multiple computer networks to interconnect and communicate with each other, which led to the development of the transfer control protocol/internet protocol (TCP/IP) in the late 1970s. At this time, the term "internetworking" was coined, eventually leading to the term "Internet" as a shorthand term for this network of networks.

[30] In the mid-1980s, NASA, the National Science Foundation (NSF) and the Department of Energy (DOE) worked on development of a successor to ARPANET and created the first multi-protocol wide area network, called the NASA Science Internet or NSI. As a high-speed, multi-protocol, international network, NSI provided connectivity to over 20,000 scientists across all seven continents. Also in the 1980s, CERN, the European Organization for Nuclear Research, installed and operated TCP/IP, first, to interconnect its internal computer systems and, then, to provide external connections to other computer systems worldwide.

The Telecommunications Act of 1996[31] represented the first major overhaul of telecommunications law since the enactment of the Communications Act. Its stated purpose was to "promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies."[32] The 1996 Act significantly deregulated U.S. telecommunications markets, eliminating regulatory barriers that had previously prevented various types of service providers from competing with one another: it opened the door for local telephone companies to provide long distance services and for long distance carriers and cable television operators to provide local phone service. Cognizant of the potential of then-emerging digital communications networks, the 1996 Act articulated that:

> the policy of the United States [is] . . . to promote the continued development of the Internet and other interactive computer services and other interactive media . . . [and] preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation . . . .[33]

The thirteen years since the Telecommunications Act was passed have witnessed significant growth and transformation in the telecommunications marketplace. Advanced wireline and, increasingly, wireless broadband network infrastructures have been (and continue to be) deployed that provide an increasingly diverse array of applications and services to both commercial and individual users, accessible over a growing variety of fixed and mobile devices. They support the clearing of billions of dollars in transactions among financial institutions, trading on exchanges, online banking, e-commerce, as well as billing and account management for many retailers and service providers; they facilitate rapid, global communications and the storage and transfer of enormous volumes of information, including proprietary business information, intellectual property, customer account and transaction information, and other personally identifiable private user information such as health records; they make an array of heretofore inaccessible information available at the user's fingertips with a few keystrokes. They have also become essential elements in the operation and management of a range of critical infrastructure functions, including transportation systems, shipping, the electric power grid, oil and gas pipelines, nuclear plants, water systems, critical manufacturing, and many others.

The capabilities of these systems have also changed the way governments at all levels do business: they enable advanced communications for law enforcement, public safety, and emergency response officials; make government more accessible (e.g., *e*-FOIA); and have led to innovative new means of delivering a wide variety of services and benefits to citizens (including motor vehicle licensing and registration, social security benefits, tax administration, and grants management). As noted above, they also support continuity of the most critical functions of national government, including command and control of the armed forces, foreign affairs, intelligence, crisis response, and national criminal investigation and law enforcement.

---

[31] Pub. L. No. 104-104, 110 Stat. 56.

[32] *Id.*

[33] 47 U.S.C. § 230(b). In connection with this policy, the 1996 Act also included a "good Samaritan" provision to protect Internet Service Providers (ISPs) from liability when they act in good faith to block or screen offensive content hosted on their systems. *Id.* § 230(c).

As dependence on these converged systems grew, users and network managers became aware of new types of vulnerabilities in the infrastructure. Moreover, the rapid emergence of the online commercial environment, the growing monetary value of transactions, and the increasing volume of sensitive information accessible online have also increased the online threat landscape by fueling the growth of organized criminal elements and other adversaries. Not only was it necessary to protect the information content, it became necessary to ensure the confidentiality of information as well as the authenticity of its sender and recipient.

Although these trends increased following the 1996 Telecommunications Act, they had already been under way for some time. Thus, by 1998, as the scope of the risk associated with these dependences expanded to encompass not only converged government communications and information systems, but also the systems supporting national critical infrastructures, policy makers began to recognize the need for an integrated effort that coupled the capabilities of government and the private sector to mitigate these risks. "Cybersecurity" emerged as a distinct policy area. Presidential Decision Directive 63 (PDD-63), signed in May 1998, established a structure under White House leadership to coordinate the activities of designated lead departments and agencies, in partnership with their counterparts from the private sector, to "eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."[34]

As these efforts matured, the White House in late 2001 augmented the structure by formally chartering the *President's Critical Infrastructure Protection Board*, an interagency body with cabinet-level representation from the departments and agencies and chaired by the Special Advisor to the President for Cyberspace Security in the NSC who was "assisted by an appropriately sized staff within the White House Office."[35] The board was charged to "recommend policies and coordinate programs for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems." This mandate also included specific responsibilities to coordinate, in consultation with relevant offices, a range of functions including: outreach to and consultation with the private sector and State and local government, information sharing, cyber incident response programs and policies, federal government research and development for information system security and emergency preparedness communications, law enforcement programs against cyber crime, international information infrastructure protection, and legislative recommendations relating to protection of information systems.[36]

This coordinating function continued until March 2003, when the White House dissolved the board and its supporting staff function incident to the creation of the Department of Homeland Security (DHS). The Homeland Security Act of 2002 (HSA) made the Department of Homeland Security responsible for coordinating national efforts to protect critical infrastructure across all sectors, including information technology and telecommunications systems. It also gave the Secretary of Homeland Security wide access to information relating to threats of terrorism against the United States and to all information concerning infrastructure or other vulnerabilities of the U.S. to terrorism.

[34] Presidential Decision Directive 63, *Critical Infrastructure Protection,* May 22, 1998, at section II.
[35] Executive Order No. 13231, *Critical Infrastructure Protection in the Information Age,* October 16, 2001 §§ 3, 7.
[36] *Id.* § 5.

From an operational standpoint, the HSA transferred to DHS responsibility for managing the National Communications System (NCS) as well as the Federal Computer Incident Response Center (FedCIRC), which had previously been operated by the General Services Administration. Within months after coming into existence, DHS established the National Cyber Security Division within its Office of Infrastructure Protection as a differentiated component to manage the Department's cyber security policy and operational responsibilities.[37] Shortly after creating the NSCD, DHS established the United States Computer Emergency Readiness Team (US-CERT) as the successor to FedCIRC, to serve as the principal cyber watch, warning, and analysis center for Federal civilian departments and agencies and an operational point of coordination with the private sector for cyber incident response.

Homeland Security Presidential Directive 7, issued in December 2003, superseded PDD-63. It reiterated U.S. policy to enhance the protection of the nation's critical infrastructure, including its cyber infrastructure. It further assigned the Secretary of Homeland Security the responsibility for coordinating the nation's overall critical infrastructure protection efforts across all sectors, working in cooperation with designated sector-specific agencies within the Executive Branch. It designated DHS as a the lead agency for the nation's Information Technology and Communications sectors, to share threat information, help assess vulnerabilities, and encourage appropriate protective action and the development of contingency plans.

Other Important Developments

Complementing these statutes affecting the structure and economic regulation of the communications marketplace, Congress has also over time enacted various laws intended to protect the public from abuses of these communications platforms and to facilitate their use in support of criminal investigations and other law enforcement purposes. The Communications Assistance for Law Enforcement Act (CALEA), enacted in 1994, amended both the Wiretap Act and ECPA. It further defined the existing statutory obligation of telecommunications carriers to assist law enforcement in executing electronic surveillance, including over wireless and digital communications systems, pursuant to court order or other lawful authorization. CALEA was intended to preserve law enforcement's ability to conduct lawful electronic surveillance over emerging digital networks while preserving public safety, the public's right to privacy, and the telecommunications industry's competitiveness.

To address the lack of criminal laws available to fight emerging computer crimes following the advent of computers as consumer electronics items in the early 1980s, Congress enacted the Comprehensive Crime Control Act of 1984, which included provisions to address the unauthorized access and use of computers and computer networks.[38] Two years later, that was followed by the Computer Fraud and Abuse Act of 1986 (CFAA). The CFAA clarified provisions in the 1984 law and also criminalized additional computer-related acts, including theft of property via computer and

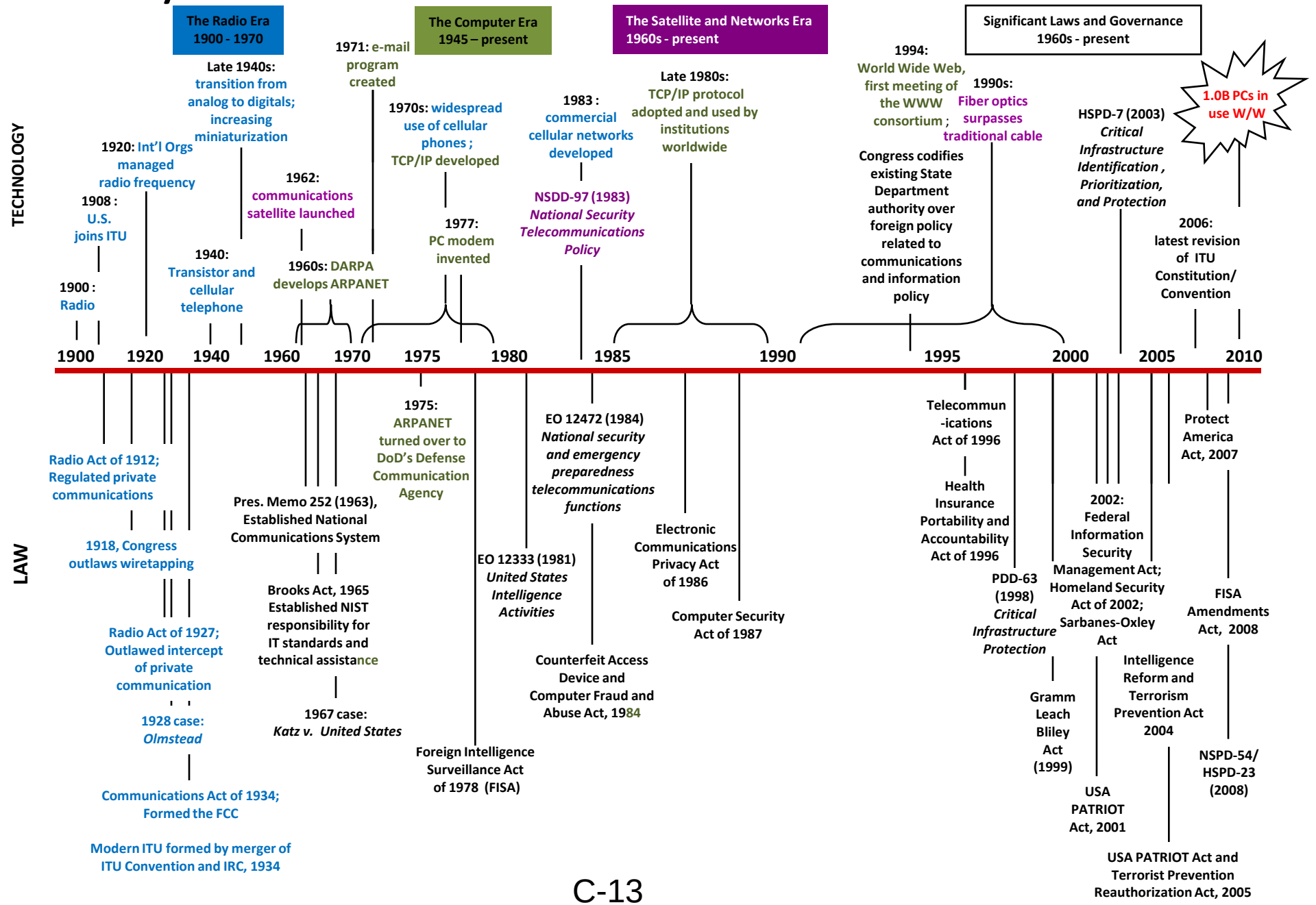
[37] In the Post-Katrina Emergency Management Reform Act, Pub. L. 109-295 (Oct. 4, 2006), 120 Stat. 1355, Congress amended the HSA to reorganize DHS, establishing an Office for Cybersecurity and Communications under a new Assistant Secretary. *Id.,* 120 Stat. 1409. This office incorporated NCSD, the Office of the Manager of NCS, and a new Office of Emergency Communications, which was also established by the statute.

[38] 18 U.S.C. § 1030.

the intentional alteration, damage, or destruction of data belonging to others.[39] The USA PATRIOT Act of 2001, passed in the aftermath of the terrorist attacks of September 11, 2001, and reauthorized in 2005, provided a range of tools to support law enforcement capabilities to combat terrorism, including enhancing law enforcement's surveillance capabilities.

Conclusion

The history of electronic communications in the United States reflects steady, robust technological innovation punctuated by government efforts to regulate, manage, or otherwise respond to issues presented by these new media, including security concerns. The iterative nature of the statutory and policy developments over time has led to a mosaic of government laws and structures governing various parts of the landscape for information and communications security and resiliency. Effectively addressing the fragmentary and diverse nature of the technical, economic, legal, and policy challenges will require a leadership and coordination framework that can stitch this patchwork together into an integrated whole.

[39] *See* http://www.usdoj.gov/criminal/cybercrime/ccmanual/01ccma.pdf.

History Informs our Future