

COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

DECEMBER 1, 2016

REPORT ON SECURING AND
GROWING THE DIGITAL ECONOMY

December 1, 2016

Dear Mr. President,

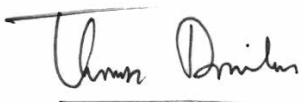
On behalf of the members of the Commission on Enhancing National Cybersecurity, we are pleased to present our final report. You charged this nonpartisan Commission with developing actionable recommendations for securing and growing the digital economy by strengthening cybersecurity in the public and private sectors. Recent events have underscored the importance and urgency of this effort.

The Commission's process was open and transparent, building on previous initiatives and the latest information from a wide range of experts and the public. Drawing on these resources, the Commission has identified six imperatives for enhancing cybersecurity, along with specific recommendations and action items supporting each imperative. Successful implementation of our recommendations will require significant commitment from both the public and private sectors and extensive cooperation and collaboration between the two. Indeed, enhancing the state of national cybersecurity will require the coordinated effort of a wide range of organizations and individuals.

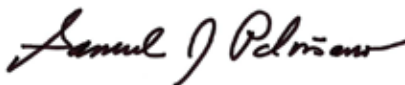
We thank you for recognizing the importance of cybersecurity and the need to safeguard our nation. We also appreciate the value of several cybersecurity-related initiatives you launched during your Administration. These efforts have led to significant progress in improving the state of cybersecurity. As you well know, there is a long way to go, and it is critical that the next Administration make cybersecurity a top priority, beginning during the transition period, so that progress can continue, accelerate, and expand. The urgency of the situation demands that the next Administration move forward promptly on our recommendations, working closely with Congress and the private sector.

It has been an honor for all of us on the Commission to be called on to help our nation to enhance its cybersecurity. We hope that this report will lead to improvements in cybersecurity that positively affect our national security and our digital economy for many years to come.

Sincerely,



Thomas E. Donilon
Chair



Samuel J. Palmisano
Vice Chair

Members of the Commission

The following 12 individuals constitute the President's Commission on Enhancing National Cybersecurity:

- **Commission Chair Thomas E. Donilon**, Vice Chair, O'Melveny & Myers; Former U.S. National Security Advisor to President Obama
- **Commission Vice Chair Samuel J. Palmisano**, Retired Chairman and CEO, IBM Corporation
- **General (Ret.) Keith B. Alexander**, Founder/CEO of IronNet Cybersecurity; Former Director of the National Security Agency; Former Founding Commander of U.S. Cyber Command
- **Ana I. Antón**, Professor and Chair of the School of Interactive Computing, Georgia Institute of Technology
- **Ajay Banga**, President and CEO, MasterCard
- **Steven Chabinsky**, Global Chair of Data, Privacy, and Cyber Security, White & Case
- **Patrick Gallagher**, Chancellor, University of Pittsburgh; Former Director, National Institute of Standards and Technology
- **Peter Lee**, Corporate Vice President, Microsoft Research
- **Herbert Lin**, Senior Research Scholar for Cyber Policy and Security, Stanford University
- **Heather Murren**, Former Commissioner, Financial Crisis Inquiry Commission; Founder, Nevada Cancer Institute; Former Managing Director, Global Consumer Products Research, Merrill Lynch
- **Joseph Sullivan**, Chief Security Officer, Uber
- **Maggie Wilderotter**, Chairman and CEO, The Grand Reserve Inn; Former Executive Chairman, Frontier Communications
- **Kiersten Todt**, Executive Director, Commission on Enhancing National Cybersecurity

Contents

| | |
|---|----|
| Executive Summary..... | 1 |
| I. The President’s Charge and the Commission’s Approach..... | 3 |
| II. The State of Cybersecurity and a Vision for the Future..... | 7 |
| III. Imperatives, Recommendations, and Action Items..... | 11 |
| Imperative 1: Protect, Defend, and Secure Today’s Information Infrastructure and Digital Networks..... | 13 |
| Imperative 2: Innovate and Accelerate Investment for the Security and Growth of Digital Networks and the Digital Economy..... | 23 |
| Imperative 3: Prepare Consumers to Thrive in a Digital Age..... | 29 |
| Imperative 4: Build Cybersecurity Workforce Capabilities..... | 33 |
| Imperative 5: Better Equip Government to Function Effectively and Securely in the Digital Age..... | 39 |
| Imperative 6: Ensure an Open, Fair, Competitive, and Secure Global Digital Economy..... | 47 |
| IV. Next Steps..... | 51 |
| Appendix 1: Imperatives, Recommendations, and Action Items..... | 53 |
| Appendix 2: List of Public Meetings and Agendas..... | 61 |
| Appendix 3: Request for Information (RFI) Submissions..... | 69 |
| Appendix 4: Executive Order 13718..... | 71 |
| Appendix 5: Cybersecurity Policy Overview..... | 75 |
| Appendix 6: Cybersecurity Legislation Overview..... | 81 |
| Appendix 7: Acronym and Abbreviation List..... | 85 |
| Appendix 8: Glossary..... | 87 |

This page intentionally left blank.

Executive Summary

Recognizing the extraordinary benefit interconnected technologies bring to our digital economy—and equally mindful of the accompanying challenges posed by threats to the security of the cyber landscape—President Obama established this Commission on Enhancing National Cybersecurity. He directed the Commission to assess the state of our nation’s cybersecurity, and he charged this group with developing actionable recommendations for securing the digital economy. The President asked that this enhanced cybersecurity be achieved while at the same time protecting privacy, ensuring public safety and economic and national security, and fostering the discovery and development of new technical solutions.

The interconnectedness and openness made possible by the Internet and broader digital ecosystem create unparalleled value for society. But these same qualities make securing today’s cyber landscape difficult. As the world becomes more immersed in and dependent on the information revolution, the pace of intrusions, disruptions, manipulations, and thefts also quickens. Technological advancement is outpacing security and will continue to do so unless we change how we approach and implement cybersecurity strategies and practices. Recent attacks in which everyday consumer devices were compromised for malicious use have made it abundantly clear that we now live in a much more interdependent world. The once-bright line between what is critical infrastructure and everything else becomes more blurred by the day.

While the threats are real, we must keep a balanced perspective. We should be able to reconcile security with innovation and ease of use. The Internet is one of the most powerful engines for social change and economic prosperity. We need to preserve those qualities while hardening it and making it more resilient against attack and misuse. Changes in policies, technologies, and practices must build on the work begun by the private sector and government, especially over the past several years, to address these issues.

Our commitment to cybersecurity must match our commitment to innovation. If our digital economy is to thrive, it must be secure. That means that every enterprise in our society—large and small companies, government at all levels, educational institutions, and individuals—must be more purposefully and effectively engaged in addressing cyber risks. They must also have greater

accountability and responsibility for their own security, which, as we now know all too well, directly impacts the cybersecurity of our country.

From its inception, this nonpartisan Commission developed a report directed both to President Obama and to the President-elect. The Commissioners, who possess a range of expertise relating to cybersecurity, reviewed past reports and consulted with technical and policy experts. The Commission held public hearings, issued an open solicitation for input, and also invited the public at large to share facts and views. It devoted attention to areas including critical infrastructure, the Internet of Things (IoT), research and development (R&D), public awareness and education, governance, workforce, state and local issues, identity management and authentication, insurance, international issues and the role of small and medium-sized businesses.

The Commission identified and considered broader trends affecting each of these topics, notably the convergence of information technologies and physical systems, risk management, privacy and trust, global versus national realms of influence and controls, the effectiveness of free markets versus regulatory regimes and solutions, legal and liability considerations, the importance and difficulty of developing meaningful metrics for cybersecurity, automated technology-based cybersecurity approaches, and consumer responsibilities. In these areas and others, the Commissioners examined what is working well, where the challenges exist, and what needs to be done to incentivize and cultivate a culture of cybersecurity in the public and private sectors.

There was much to readily agree on, including the growing convergence and interdependencies of our increasingly connected world; the need for greater awareness, education, and active stakeholder engagement in all aspects of cybersecurity, from developers and service providers to policy makers and consumers; the ways in which small- and medium-sized companies face additional pressures and limitations in addressing cybersecurity and the importance of remedying that situation, especially in light of their role in the supply chain; and the need, from both operational and mission perspectives, to clarify the federal government’s roles and responsibilities.

It was also evident that most solutions require joint public-private action. Every enterprise in our society—large and small

companies, government at all levels, educational institutions, and individuals—must be more purposefully and effectively engaged in addressing cyber risks. They must be equipped to understand the role they play in their own security and how their actions directly impact the cybersecurity of the nation more broadly.

Other areas required more consideration:

- how best to incentivize appropriate cybersecurity behaviors and actions and how to determine if or when requirements are called for;
- who should lead in developing some of the most urgently needed standards and how best to assess whether those standards are being met;
- what is the feasibility of better informing consumers, for example, through labeling and rating systems;
- which kinds of research and development efforts are most needed and at what cost;
- how to project the right number of new cybersecurity professionals our economy needs and how to choose among different approaches for attracting and training the workforce at all levels; and,
- what the roles and relationships of senior federal officials should be and how best to ensure that they not only have the right authorities but are empowered to take the appropriate actions.

From these discussions, some firm conclusions emerged. Partnerships—between countries, between the national government and the states, between governments at all levels and the private sector—are a powerful tool for encouraging the technology, policies, and practices we need to secure and grow the digital economy. The Commission asserts that the joint collaboration between the public and private sectors before, during, and after a cyber event must be strengthened. When it comes to cybersecurity, organizations cannot operate in isolation.

Resilience must be a core component of any cybersecurity strategy; today's dynamic cyber threat environment demands a risk management approach for responding to and recovering from an attack.

After building on those points of agreement and identifying foundational principles, the Commissioners organized their

findings into six major imperatives, which together contain a total of 16 recommendations and 53 associated action items.

The imperatives are:

1. Protect, defend, and secure today's information infrastructure and digital networks.
2. Innovate and accelerate investment for the security and growth of digital networks and the digital economy.
3. Prepare consumers to thrive in a digital age.
4. Build cybersecurity workforce capabilities.
5. Better equip government to function effectively and securely in the digital age.
6. Ensure an open, fair, competitive, and secure global digital economy.

A table detailing these imperatives and their associated recommendations and action items is included in Appendix 1. The groupings should not be viewed as distinct and isolated categories; indeed, a number of recommendations apply to more than the imperative under which they first appear. The text notes when action items are particularly relevant to other imperatives. This structure reflects the interdependent nature of our digital economy, where steps taken to improve the cybersecurity of one enterprise can meaningfully improve the posture and preparedness of others.

Each recommendation is designed to have a major impact, and each action item is meant as a concrete step toward achieving that impact. Many require a commitment of financial resources far above the level we see today. Some are directed at government, some at the private sector, and many at both. Some call for entirely new initiatives, while others call for building on promising efforts currently under way.

Acknowledging the urgency of the challenges facing our nation, the Commission determined that most recommendations can and should begin in the near term, with many meriting action within the first 100 days of the new Administration. All of these recommendations and actions highlight the need for the private sector, government, and American public to recognize cybersecurity as an integral part of our welfare with serious implications for our country's national and economic security and our prospects to maintain a free and open society.

I. The President's Charge and the Commission's Approach

No one—not even the visionaries who created the Internet a half century ago—could have imagined the extent to which digital connectivity would spur innovation, increase economic prosperity, and empower populations across the globe. Indeed, the Internet's origins in the defense community are today almost an afterthought, as its explosive growth has given it a dramatically different shape. Its creators could not have dreamed of the way and the extent to which our national and global economies have thrived, how innovations have been enabled, and how our population has been empowered by our digital connectivity.

With these benefits and transformational changes have come costs and challenges. The interconnectedness and openness that the Internet, digital networks, and devices allow have also made securing our cyber landscape a task of unparalleled difficulty. As the world becomes more dependent on the information revolution, the pace of intrusions, disruptions, manipulations, and thefts also quickens. Beyond the resulting economic losses and national security threats, our privacy, civil liberties, and constitutional rights—even the voting system that underlies our democracy—all become vulnerable. For now, technological advancement continues to outpace security and will continue to do so unless shifts in our cybersecurity strategies—and how well we implement those strategies—are made.

While the threats are real, they also should not cause us to overreact. It is important to keep a balanced perspective. We should be able to reconcile security with innovation. The Internet is an engine for social change and economic prosperity, and we need to preserve those qualities while making it more resilient. Changes in policies, technologies, and practices must build on the work begun by the private sector and government, especially over the past several years, to address these issues. This Commission sees how those positive actions are taking hold in the marketplace and in the public sector. One important step in the right direction is the notable increase in awareness about cybersecurity risks, from the boardroom to the family room.

But clearly, many more steps have to be taken. Our commitment to cybersecurity must be commensurate with, and not lag behind, our commitment to innovation. To facilitate the growth and security of the digital economy, every enterprise of our society—

large and small companies, government at all levels, educational institutions, and individuals—must be more purposefully and effectively engaged in addressing cyber risks. They must also have greater accountability and responsibility for their own security, which directly impacts the entire country's state of cybersecurity.

The President charged this Commission with developing actionable recommendations for securing the digital economy in the near term and into the future. The President asked the Commission to identify what is working well, where challenges exist, and what more needs to be done, with a vision toward incentivizing and cultivating a culture of cybersecurity in the public and private sectors. This enhanced cybersecurity is to be achieved while:

- protecting privacy;
- ensuring public safety and economic and national security;
- fostering discovery and development of new technical solutions; and,
- bolstering partnerships between federal, state, and local governments and the private sector in developing, promoting, and using cybersecurity technology, policies, and best practices.

The Commission and How It Gained Its Insights

To carry out his executive order,¹ President Obama appointed 12 people to this nonpartisan Commission—four recommended by leaders of both parties in the Senate and the House of Representatives and the others selected by the President. The members of the Commission have experience in numerous sectors of society and varied expertise in many areas, including the federal government, public policy, research and development, law enforcement, academia, consumer matters, and the management of large enterprises.

¹ <https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity>. For the text of Executive Order 13718, see Appendix 4.

Several federal agencies provided subject matter experts and other staff to assist the Commission with information gathering and analysis. These include the Department of Commerce's National Institute of Standards and Technology (NIST), which served as the secretariat for this Commission; the Department of Homeland Security (DHS); Department of Defense (DoD); the Department of Justice (DOJ); the General Services Administration (GSA); and the Department of the Treasury. All staff members worked at the direction of the Commission rather than as representatives of their agencies.

The President encouraged the Commission to address hard questions and think outside current norms. It did so by drawing on the members' own expertise and by reaching out broadly across society to gain insights and develop meaningful recommendations that would fulfill the Commission's mandate. The Commission took into account previous studies and reports, recent initiatives by the private and public sectors, and major cybersecurity-related incidents occurring even as the Commission conducted its work.

To gather additional information on these topics, the Commission held six public meetings throughout the country where subject matter experts from many domains spoke about the past, current, and future state of cybersecurity and the digital economy.² Members of the public also had opportunities to provide input to the Commission, both by speaking during comment periods at Commission meetings and by sending written submissions in response to an open request for information (RFI).³

The Commission reviewed numerous past reports prepared by various federal executive and legislative branch organizations as well as by private-sector organizations. The reports ranged from broad-based analyses of the state of cybersecurity across the nation to highly targeted analyses of specific areas, such as research and development and U.S. military needs.

Many of the recommendations in those past reports focused on actions to be taken by the federal government for the benefit of the federal government. Common themes included making organizational changes in support of better decision making, better

tracking of agency activities and incidents, and better public-sector information exchange.

Past reports also contained several recommendations that, while arguably in the best interest of the security of the nation, were not realistic, given the market forces at the time they were written or in the present day. The Commission asserts that market forces and the needs of private businesses, governments, households, and individuals must be taken into account when putting forth recommendations. This Commission's recommendations balance ambitious, long-term goals with practical and pragmatic solutions.

Areas of Focus

From the text of the executive order, the Commission initially identified eight cybersecurity topics to study:

- federal governance
- critical infrastructure
- cybersecurity research and development
- cybersecurity workforce
- identity management and authentication
- Internet of Things
- public awareness and education
- state and local government cybersecurity

The Commission added two topics to this list: insurance and international issues. The Commission also took into account broader trends and issues affecting each of these topics, notably the convergence of information technologies and physical systems, risk management, privacy and trust, global versus national realms of influence and controls, free market and regulatory regimes and solutions, legal and liability considerations, the difficulty in developing meaningful metrics of cybersecurity, and automated technology-based cybersecurity approaches and consumer responsibilities.

Foundational Principles

The Commission identified the following ten principles that helped shape its recommendations to secure and grow the digital economy:

1. The growing convergence, interconnectedness, interdependence, and global nature of cyber and physical systems means that cybersecurity must be better managed in all contexts—international, national, organizational, and individual.

2 See Appendix 2 for the full list of Commission public meetings and meeting agendas as well as URLs pointing to panelist statements and meeting minutes.

3 See Appendix 3 for more information on the RFI, including a URL for a page containing links to copies of all RFI submissions.

2. As the global leader for innovation, the United States must be a standard-bearer for cybersecurity. This leadership requires investing in research and collaborating with other nations, including on international cybersecurity standards.
3. The federal government has the ultimate responsibility for the nation's defense and security and has significant operational responsibilities in protecting the nation's rapidly changing critical infrastructure. The government also has cyber mission roles that need to be clarified, including better defining government (including individual agency) roles and responsibilities, and addressing missing or weak capabilities, as well as identifying and creating the capacity that is needed to perform these activities.
4. Private sector and government collaboration before, during, and after an event is essential in creating and maintaining a defensible and resilient cyber environment.
5. Responsibility, authority, capability, and accountability for cybersecurity and cyber risk management should be explicit and aligned within every enterprise's risk management and governance strategies.
6. Effective cybersecurity depends on consumer and workforce awareness, education, and engagement in protecting their digital experience. This effort must be a continuous process and advance individuals' understanding and capabilities as vital participants in shaping their own—and the nation's—cybersecurity. Nevertheless, to the maximum extent possible, the burden for cybersecurity must ultimately be moved away from the end user—consumers, businesses, critical infrastructure, and others—to higher-level solutions that include greater threat deterrence, more secure products and protocols, and a safer Internet ecosystem.
7. Because human behavior and technology are intertwined and vital to cybersecurity, technologies and products should make the secure action easy to do and the less secure action more difficult to do.
8. Security, privacy, and trust must be primary considerations at the outset when new cyber-related technologies and policies are conceived, rather than auxiliary issues to be taken into account after they are developed. Improved privacy and trust, boosted by transparency and accountability, will contribute to the preservation of civil liberties.
9. Despite their often-constrained resources, small and medium-sized businesses are essential stakeholders in any effort to enhance cybersecurity—particularly in light of their role in the supply chain—and their needs must be better addressed.
10. The right mix of incentives must be provided, with a heavy reliance on market forces and supportive government actions, to enhance cybersecurity. Incentives should always be preferred over regulation, which should be considered only when the risks to public safety and security are material and the market cannot adequately mitigate these risks.

Imperatives, Recommendations, and Action Items

Recognizing the increasing intensity and variety of risks faced by this nation, and relying on the foundational principles cited above, the Commission identified the top six imperatives for enhancing cybersecurity, which are described in Chapter III.

The Commission also identified 16 recommendations and 53 related actions that are both practical and ambitious and will enhance U.S. cybersecurity. Like cybersecurity itself, these recommendations should not be considered in isolation: there is considerable cross-pollination of ideas among them. For instance, although the Commission has singled out an international imperative with its own recommendations, international aspects are woven throughout the recommendations. The same holds true for recommendations that appear in imperatives addressing the Internet and digital networks of today versus those of the future. Additionally, it is important to note that the prioritization of cybersecurity requires a long-term commitment and an increased investment of resources in both the public and private sectors.

This page intentionally left blank.

II. The State of Cybersecurity and a Vision for the Future

Computing technologies have enormous potential to improve the lives of all Americans. Each day we see new evidence of how transformative these technologies can be, and the ways they can positively affect our economy and our quality of life in the workplace. We live in a digital economy that helps us work smarter, faster, and more safely. Change is not limited just to our workplaces, of course. Our lives are enriched by digital devices and networks and by the innovators who have found creative ways to harness technology.

Still, our digital economy and society will achieve full potential only if Americans trust these systems to protect their safety, security, and privacy. A wave of highly publicized incidents over the past several years has brought the importance of cybersecurity into focus for policy makers, private-sector leaders, and the American people. Concerns that malicious cyber activity could have a significant national impact on critical infrastructure, such as the power grid and the financial system, continue to grow even as we achieve successes in bolstering cybersecurity.

The Commission examined key cybersecurity issues, identified the main challenges to achieving cybersecurity and securing the digital economy, and offers the following broad findings:

1. Technology companies are under significant market pressure to innovate and move to market quickly, often at the expense of cybersecurity. In many industries, being “first to market” continues to take priority over being “secure to market.” Security features later may be added to subsequent versions of a product, but doing so results in a product with inferior security compared to one that has security integrated into its initial design and development of a new product. The adoption of secure coding practices, as well as the development and use of better tools, can significantly reduce the number of exploitable vulnerabilities in software products. However, these practices and the need to develop and deploy tools take time and money to implement and can slow down the pace of development and release. Both larger and smaller companies grapple with this issue; in many respects, smaller companies have even less flexibility in light of market pressures and constraints in accessing appropriate expertise.

2. Organizations and their employees require flexible and mobile working environments. The days of employees working only at an office using an organization-issued desktop computer fully managed by the organization are largely over. Market forces and employee demands have made “bring your own device” the de facto option in many workplaces. Few organizations are able to function without connecting to vendors, customers, and partners in multiple global supply chains. Organizations no longer have the control over people, locations, networks, and devices on which they once relied to secure their data. Mobile technologies are heavily used by almost every organization’s employees, yet security for mobile devices is often not considered as high a priority as security for other computing platforms. In short, the classic concept of the security perimeter is largely obsolete.

3. Many organizations and individuals still fail to do the basics. Malicious actors continue to benefit from organizations’ and individuals’ reluctance to prioritize basic cybersecurity activities and their indifference to cybersecurity practices. These failures to mitigate risk can and do allow malicious actors of any skill level to exploit some systems at will.

4. Both offense and defense adopt the same innovations. For example, near-term advances in machine learning, automation, and artificial intelligence have the potential to address some of the persistent problems in cybersecurity, yet criminals and nation-state adversaries undoubtedly will find malicious uses for these capabilities as well. Likewise, quantum computing has the potential to render useless some of the encryption technology we rely on today.

5. The attacker has the advantage. Some threats against organizations today are from teams composed of highly skilled attackers that can spend months, if not years, planning and carrying out an intrusion. These teams may be sponsored by nation-states or criminal organizations, hacktivist groups, and others. Less skilled malicious actors can easily purchase attack toolkits, often with technical support, enabling them to readily participate in criminal activities. A security team has to protect thousands of devices while a malicious actor needs to gain access to only one. The cost to attack a system is only a fraction of the cost to defend it.

6. **Technological complexity creates vulnerabilities.**

Complexity today is affected by the continuously changing and interdependent environment, the increased number of mobile clients, and the compressed time available from when a product is first conceptualized to when it goes to market. As the size and complexity of software and computing systems continue to grow, more vulnerabilities are exposed and introduced into environments that are increasingly difficult to manage. As more and more programs and systems are expected to be able to integrate seamlessly with each other, vulnerabilities are created when and where they connect, exponentially expanding opportunities for risk. The constant cycle of updating software (often to address security flaws) can introduce new vulnerabilities and increase system complexity. Complexity also arises from the connection of Internet of Things (IoT) devices that have both antiquated software and newly generated hardware and software.

7. **Interdependencies and supply chain risks abound.** Our way of life has become reliant on complex webs of interconnected infrastructure with many interdependencies. The fast-moving shift to increased connectivity, oversimplified in the term “Internet of Things”, along with its many vulnerabilities and much more decentralized structure, has introduced an entirely new component into the equation. Communities, businesses, and industries may not be fully aware of their interdependencies, many of which involve small and large companies that contribute to the supply chain that develops products. Likewise, elements of critical infrastructure, such as the electric grid and communications systems, are dependent on other sectors for their own operation.

8. **Governments are as operationally dependent on cyberspace as the private sector is.** Governments face cybersecurity challenges that the private sector does not. These challenges include a large legacy information technology base, difficulty competing for cybersecurity talent, a procurement process that is not built for the digital age, and an inability to plan future investment beyond the horizon and functionality of the legislative budget cycle.

9. **Trust is fundamental.** The success of the digital economy ultimately relies on individuals and organizations trusting

computing technology and trusting the organizations that provide products and services and that collect and retain data. That trust is less sturdy than it was several years ago because of incidents and successful breaches that have given rise to fears that corporate and personal data are being compromised and misused. Concern is increasing, too, about the ability of information systems to prevent data from being manipulated; the most recent national election heightened public awareness of that issue. In most cases, data manipulation is a more dangerous threat than data theft.

In reviewing and analyzing the current state of cybersecurity, the Commission was mindful that much of the technology landscape in which cybersecurity policy is made is evolving rapidly. Indeed, technology advances almost always outpace policy developments. These scientific and technical advances change how our nation does business. They introduce new challenges and improve cybersecurity, but many organizations, if not most, rely on policies, frameworks, and standards that have not been updated to take these technological innovations into account.

For example, the emergence of communications networks for household devices, transportation systems, public works, and all manner of business systems offers immense opportunities for innovation and efficiency, but it also presents significant security challenges. In the near future, an average household may have more connected devices than a medium-sized business enterprise today.⁴ Many people may also choose (or be medically required) to connect numerous devices to their own bodies. The IoT facilitates linking an incredible range of devices and products to each other and the world. Although this connectivity has the potential to revolutionize most industries and many facets of everyday life, the possible harm that malicious actors could cause by exploiting these technologies to gain access to parts of our critical infrastructure, given the current state of cybersecurity, is immense. In September and October 2016, we saw firsthand evidence of this vulnerability created by interdependencies when IoT devices, built for basic consumer use, were used to create

4 “Gartner Says a Typical Family Home Could Contain More Than 500 Smart Devices by 2022,” Gartner press release, September 8, 2014, <http://www.gartner.com/newsroom/id/2839717>.

large-scale botnets—networks of devices infected with self-propagating malware—that executed crippling distributed denial-of-service (DDoS) attacks.⁵

Recent Improvements and a Vision for the Future

The Commission takes note of positive changes in both the private and public sectors' approach to cybersecurity. In response to recurring challenges, companies have begun to prioritize cybersecurity, sometimes reflected in increased investment in their own cybersecurity—though it is important to recognize that an increase in spending does not necessarily result in an increase in security. The global market for cybersecurity products has attracted many entrepreneurs, technologists, and venture capitalists in Silicon Valley and other hubs of innovation. The key point is to ensure that this increase in innovation aligns with the needs of the digital economy. The boards of public companies and their shareholders have begun to take a strong interest in cyber threats as a tangible business risk, factoring cybersecurity and associated risks and needs into their decisions on what markets to enter, what information technology products to purchase, and what companies to do business with or to acquire.

The Obama Administration has launched a series of aggressive initiatives to spur federal agencies to improve their cybersecurity readiness and performance. To play catch-up with the private sector, federal agencies have been directed to improve their governance, systems, and personnel to advance cyber-related security, as exemplified by the 2015 series of “cyber sprints,”⁶ which were executed in response to the Office of Personnel Management (OPM) breach. While the results of the cyber sprints were encouraging, it should not have taken the largest data breach in U.S. government history to trigger these actions. It is important to note that state governments have brought new energy to dealing with their own cybersecurity challenges and are making noteworthy improvements in resource-constrained environments, although their progress has been slower than desired.

5 US-CERT, “Alert (TA-288a): Heightened DDoS Threat Posed by Mirai and Other Botnets,” October 14, 2016, last revised October 17, 2016, <https://www.us-cert.gov/ncas/alerts/TA16-288A>

6 Tony Scott, “Factsheet: Enhancing and Strengthening the Federal Government’s Cybersecurity,” White House blog, June 17, 2015, <https://www.whitehouse.gov/blog/2015/06/17/fact-sheet-enhancing-and-strengthening-federal-government-s-cybersecurity>.

Cybersecurity is now an explicit consideration as organizations in the private sector and at all levels of government review their workforce readiness and needs. We are not yet seeing consumer demands for cybersecurity and privacy protections as forces influencing the market, but the increase in incidents coupled with a better understanding about the risks and relative security of various products and services may soon change that. The Commission expects companies and other organizations to be incentivized to acknowledge cybersecurity concerns as more companies offer cyber insurance policies, which will likely take into account a company’s cybersecurity risk management practices when deciding whether to underwrite a risk and when setting premium levels.

Companies, large and small, as well as government agencies and other organizations now have more tools at their disposal to assess and take action to better understand and respond to cyber risks. The *Framework for Improving Critical Infrastructure Cybersecurity*,⁷ better known as the Cybersecurity Framework, is a case in point. Called for by a presidential executive order in 2013 and produced a year later in a collaborative private–public effort, this voluntary framework is now being used by organizations of all sizes and types across the economy to assess and prioritize cyber risks and the actions to reduce them. Once organizations are enabled to better manage those risks, they can make informed decisions about how to apply scarce resources to yield the greatest value. The Framework is being adopted by federal and state agencies and by other organizations around the country, and it is garnering interest in other countries. The Framework is a successful example of an innovative public–private solution; government convened industry to create the Framework.

That type of collaboration also must be achieved in the areas of trust and privacy. In the near future, the United States must establish as a norm that technology reliably safeguards sensitive data, such as financial information, health records, and proprietary corporate information, including intellectual property. We need technology that protects the privacy of individuals while still making it possible to provide consumers and companies with immediate access to products and services on demand, even under adverse conditions. The Commission envisions a future in which technology can be prevented from causing physical harm to people or property, even if someone attacks a physical or digital network.

7 Available at <https://www.nist.gov/cyberframework>.

America prides itself on fostering the individual entrepreneur, the independent and creative spirit, and the competitor who stands above all others. When it comes to tackling the host of cybersecurity challenges, we need those qualities—but we need joint efforts, collaboration, and cooperation even more. Government and industry each have different strengths and limitations in their cybersecurity capabilities. Mechanisms that clearly define public–private collaboration, joint planning, and coordinated response before, during, and after an event are critical and must be effectively developed.

No technology comes without societal consequences. The challenge is to ensure that the positive impacts far outweigh the negative ones and that the necessary trade-offs are managed judiciously. In doing so, we can and must manage and significantly lower cybersecurity risks while at the same time protecting privacy and other civil liberties. We must also put in place forward-thinking, coherent, and cohesive policies, developed in a transparent process, that enable our institutions and our individuals to innovate and take advantage of the opportunities created by new technology.

It is against this backdrop of current challenges and a vision for a more secure future that the Commission members have developed this report’s imperatives and recommendations.

This Commission was charged with developing recommendations for ensuring the growth and security of the digital economy, today and into the future. Identifying underlying goals and principles as a basis for those recommendations was important to the Commission’s approach. So too was developing top-level imperatives and prioritizing specific actions to make the recommendations actionable.

The following pages describe those imperatives, recommendations, and action items (presented in a table in Appendix 1). They are based on input from private- and public-sector experts and the Commissioners themselves and reflect a consensus among members of this Commission.

III. Imperatives, Recommendations, and Action Items

The Commission conducted an in-depth review of the areas called out in Executive Order 13718 chartering this work. They are described in Chapter I. All of these topics are addressed in the imperatives, recommendations, and action items.

To focus on the most important areas and assist in the presentation of its recommendations, the Commission identified six priority imperatives under which 16 recommendations appear.

The imperatives are:

1. Protect, defend, and secure today's information infrastructure and digital networks.
2. Innovate and accelerate investment for the security and growth of digital networks and the digital economy.
3. Prepare consumers to thrive in a digital age.
4. Build cybersecurity workforce capabilities.
5. Better equip government to function effectively and securely in the digital age.
6. Ensure an open, fair, competitive, and secure global digital economy.

Each recommendation includes one or more explicit action items. The groupings should not be viewed as distinct and isolated categories; indeed, some recommendations apply to more than the imperative under which they first appear. The text notes when specific action items under one imperative are particularly relevant to another. This structure reflects the nature of cybersecurity, where issues and actions cross sectors and where steps taken to meet the needs of one organization or sector can add broader value in addressing other issues and in helping to address other requirements. Recommendations pertaining to smaller companies or international actions, for example, are included in multiple imperatives.

Each action item ends with an indication of when the Commission believes the work should commence. The Commission discussed short-, medium-, and long-term time frames. Two years is the time frame for high-priority actions that could be achieved in the near term, including those on which the Administration could act and meet the Commission's goals by executive order or administrative action. Five years is the medium-term target for actions that likely would require action by both the Administration and Congress or require additional information, analysis, and

extensive consultation with other stakeholders—including regulatory changes.

Ultimately, as it recognized the urgency of the challenges confronting the nation, the Commission determined that most of the action items should begin in the short term, with some deserving action within the first 100 days of the new Administration, but none was determined to be long-term.

Descriptions of the imperatives, recommendations, and action items follow.

This page intentionally left blank.

Imperative 1: Protect, Defend, and Secure Today's Information Infrastructure and Digital Networks

The Challenge and Way Forward

Our interconnections and interdependencies are becoming more complex and now extend well beyond critical infrastructure (CI). These interconnections reduce the importance of the CI label, because, by association, all dependencies may be critical. As these linkages grow, so does the need to consider their associated risks. This convergence, combined with increased cybersecurity awareness, creates a unique opportunity to change our current approach to better protect the digital economy. Indeed, we know a great deal about measures that would enhance cybersecurity, and their implementation is urgently needed today.

We need to recognize that neither the government nor the private sector can capably protect systems and networks without extensive and close cooperation. Critical infrastructure owners and operators deserve clearer guidance and a set of common understandings on how government responsibilities, capabilities, and authorities can lead to better collaboration and joint efforts in protecting cyberspace.

Today, it is widely assumed and expected that the private sector is responsible for defending itself in cyberspace regardless of the enemy, the scale of attack, or the type of capabilities needed to protect against the attack. That assumption is problematic. The government is—and should remain—the only organization with the responsibility and, in most cases, the capacity to effectively respond to large-scale malicious or harmful activity in cyberspace caused by nation-states, although often with the assistance of and in coordination with the private sector.

A large portion of network interactions on the Internet are known to be harmful to the network. Most involve either known malware or packets that are clearly coming from a botnet or denial-of-service attack. Many of these interactions are relatively easy to identify and separate from legitimate traffic, and some organizations in the Internet and communications ecosystem are taking steps to reduce them. However, current business practices, policies, and technology can actually impede efforts to reduce these harmful interactions.

Stronger authentication of identities for interactions that require such proof must also be a key component of any approach for enhancing our nation's cybersecurity. Identity, especially the use of passwords, has been the primary vector for cyber breaches—and the trend is not improving despite our increased knowledge and awareness of this risk. Our reliance on passwords presents a tempting target for malicious actors. Despite the technical and demonstrated real-life success of a variety of novel approaches for improving identity management, individual users and the nation are still lagging significantly. Consequently, we are making it too easy for those who seek to do harm, whether they be nation-states, well-organized criminal groups, or online thieves. As detailed below, the Commission believes that the shared goal of both the public and private sectors should be that compromises of identity will be eliminated as a major attack vector by 2021.

Recommendation 1.1: The private sector and the Administration should collaborate on a roadmap for improving the security of digital networks, in particular by achieving robustness against denial-of-service, spoofing, and other attacks on users and the nation's network infrastructure.

Many organizations in the Internet and communications ecosystem,⁸ including network, edge, and content providers, are positioned to deliver the nation more effective and efficient cybersecurity. This enhanced cybersecurity would improve the agility of mitigation and response in the face of malicious activity, by moving the security problem further away from end users and organizations that do not specialize in cybersecurity (including many smaller companies). To achieve the desired outcome, there must be increased protection, fewer interruptions, and less damage from large-scale attacks on core network functionality; the federal government and private sector must commit to launching a major, multiyear joint initiative. They must team

8 For discussion of the Internet and communications ecosystem, see the Communications Security, Reliability and Interoperability Council (CSRIC) IV, "Cybersecurity Risk Management and Best Practices Working Group 4: Final Report," March 2015, https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

together to address the problems that plague our Internet-based communications now, because these problems will undoubtedly loom larger in the future.

The Administration should focus first on mitigating and, where possible, eliminating denial-of-service attacks, particularly those launched by botnets. It should then expand its scope to other attacks on Internet infrastructure, including the Domain Name System. This effort would build on previous initiatives, such as “Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment and Botnets and Related Malware.”⁹

Action Item 1.1.1: *The President should direct senior federal executives to launch a private–public initiative, including provisions to undertake, monitor, track, and report on measurable progress in enabling agile, coordinated responses and mitigation of attacks on the users and the nation’s network infrastructure.*
(SHORT TERM)

The Department of Commerce, in consultation with all other appropriate departments and agencies, should undertake a multi-stakeholder process that focuses on mitigating the impact of botnets, including denial-of-service attacks, and then expand to address other malicious attacks on users and the network infrastructure, such as the Domain Name System. This effort should build on previous initiatives, such as “Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment and Botnets and Related Malware” and those advanced by the Industry Botnet Group. Specifically, this effort would identify the actions that can be taken by organizations responsible for the Internet and communications ecosystem to define, identify, report, reduce, and respond to attacks on users and the nation’s network infrastructure. This initiative should include regular reporting on the actions that these organizations are already taking and any changes in technology, law, regulation, policy, financial reimbursement, or other incentives that may be necessary to support further action—while ensuring that no participating entity obstructs lawful content, applications, services, or nonharmful devices, subject to reasonable network management.

⁹ <https://www.ntia.doc.gov/federal-register-notice/2011/models-advance-voluntary-corporate-notification-consumers-regarding-ill>.

Recommendation 1.2: As our cyber and physical worlds increasingly converge, the federal government should work closely with the private sector to define and implement a new model for how to defend and secure this infrastructure.

To prevent destruction and degradation of infrastructure, the private sector and government must jointly and continuously address cybersecurity risk. To date, much of this effort has been focused primarily on cybersecurity incident response. Moving forward, our collective effort must focus also on all stages of operations to protect and defend networks, as well as to ensure resilience and swift recovery through joint planning and training and coordinated responses. This collaboration must occur continuously as threats are discovered, and information must be exchanged throughout the prevention and detection of, and the response to, an incident.

The private sector and government must team up to plan, exercise, and otherwise prepare in a way that takes advantage of their respective capabilities and their real-time information about malicious actors, adversaries, threats, and vulnerabilities. Companies in the private sector should be encouraged to share with the government information about any large-scale threat that they detect in their systems so that the government and industry can coordinate an appropriate response against that adversary. Conversely, government may have actionable intelligence that it should share to aid companies in planning and preparation for managing their cyber risk.

Action Item 1.2.1: *The President should create, through executive order, the National Cybersecurity Private–Public Program (NCP³) as a forum for addressing cybersecurity issues through a high-level, joint public–private collaboration.*
(SHORT TERM)

The main focus of this group would be to identify clear roles and responsibilities for the private and public sectors in defending the nation in cyberspace. It should address attribution, sharing of classified information, and training on how government conducts itself with industry, including rules of engagement and international engagement. The group should propose an approach—including recommendations on the authorities and rules of engagement needed—to enable cooperative efforts between the government and private sector to protect the nation, including cooperative operations, training, and exercises. Their focus should not be limited to nation-state and terrorist actors

but should also include hackers and cyber criminals. Like the President's Intelligence Advisory Board, the NCP³ should report directly to the President—in this case, through the recommended Assistant to the President for Cybersecurity. (See *Imperative 5, Action Item 5.4.1.*)

The NCP³ should be composed of individuals that have the necessary seniority and influence in the government and private-sector to jointly defend the nation in cyberspace, particularly against committed nation-state threat actors.

Action Item 1.2.2: *The private sector and Administration should launch a joint cybersecurity operation program for the public and private sectors to collaborate on cybersecurity activities in order to identify, protect from, detect, respond to, and recover from cyber incidents affecting critical infrastructure (CI).*

(MEDIUM TERM)

The government must address the convergence of CI with the IoT to ensure security and continuity of government. We must have a common understanding of what the government should do in response to cyber attacks targeting our CI, particularly those executed by a nation-state. We also need to identify and define clear responsibilities, authorities, and rules of engagement for both public and private organizations.

The government—including federal and state, local, tribal, and territorial (SLTT) agencies—and the private sector need a repeatable, consistent process for jointly evaluating potentially significant cyber incidents and assessing appropriate deterrence, prevention, response, and mitigation efforts from a legal, policy, national security, and business process perspective. Key aspects of any collaborative defensive effort between the government and private sector include coordinated protection and detection approaches to ensure resilience; fully integrated response, recovery, and plans; a series of annual cooperative training programs and exercises coordinated with key agencies and industry; and the development of interoperable systems.

DHS, DOJ (including the Federal Bureau of Investigation's [FBI's] InfraGard and Domestic Security Alliance Council programs), the Department of Defense (DoD), and other sector-specific agencies (SSAs) should develop sector-specific collaborative security operations programs with their private-sector counterparts as well as with state governments, which have an important role in CI protection and operation. DoD's deliberate planning process

could serve as a model for this effort. These programs would move beyond tabletop exercises and seek to establish public–private joint collaboration by examining specific cyber protection and detection approaches and contingencies, testing them in a simulation environment, and developing joint plans for how the government and private sector would execute coordinated protection and detection activities, responding together, in alignment with the National Cyber Incident Response Plan. This effort should include SLTT planners when appropriate. It should also seek to define subsector roles within each CI sector.

Action Item 1.2.3: *The federal government should provide companies the option to engage proactively and candidly in formal collaboration with the government to advance cyber risk management practices and to establish a well-coordinated joint defense plan based on the principles of the Cybersecurity Framework.* (SHORT TERM)

Even though closer and more substantive public–private sharing of risk management practices shows great promise in improving overall cybersecurity, this approach continues to be hindered by companies' concerns about increasing their exposure to legal actions. To address these impediments to helpful collaboration, DHS should work with industry to identify changes in statutes, regulations, or policies that would encourage participating companies to more freely share information about their risk management practices by protecting relevant documents, communications, or deliberations from:

- public disclosure under Freedom of Information Act (FOIA) or state transparency laws;
- discovery in civil litigation;
- use in regulatory enforcement investigations or actions;
- use as record evidence in regulatory rule-making processes; and,
- waiver of attorney–client privilege.

These protections should be implemented under the statutory Protected Critical Infrastructure Information protections administered by DHS.¹⁰ Implementation should include consideration of how to protect personal privacy, trade secrets, and other confidential information, such as by using Privacy

¹⁰ Department of Homeland Security, "Protected Critical Infrastructure Information (PCII) Program," August 30, 2016, <https://www.dhs.gov/pcii-program>.

Impact Assessments, where feasible. Using the Cybersecurity Framework approach as a basis, regulatory agencies should adopt policies that incorporate protections into their engagements with regulated entities. Furthermore, Congress should pass legislation updating and expanding these protections beyond critical infrastructure sectors and regulated entities.

Action Item 1.2.4: *Federal agencies should expand the current implementation of the information-sharing strategy to include exchange of information on organizational interdependencies within the cyber supply chain.* (SHORT TERM)

While some private-sector organizations are diligent in addressing cyber risks to and through their cyber supply chains, many others either are unaware of the risks or do not have the information and resources necessary to implement an organizationally integrated and robust cyber supply chain risk management program. Smaller organizations with fewer resources and often with less sophisticated cybersecurity capabilities are sometimes left woefully underprepared to address interdependency and supply chain risks. The increasing digital connectedness of organizations means there is a growing risk to the nation through the weak links in the supply chains in the industries all around us.

To address supply chain risk due to organizational interdependencies (such as across purchasers and suppliers), NIST should conduct further research and publish guidance. This research should identify methods that assess the nature and extent of organizational interdependencies, quantify the risks of such interdependencies, and support private-sector measurement against standards of performance. This guidance should include but not be limited to the metrics that emerge from the NCP³ Cybersecurity Framework Metrics Working Group (see *Action Item 1.4.1*). DHS, the FBI, and DoD should expand existing information-sharing networks to enable the development of a toolkit that supports this NIST guidance for use by private-sector organizations, including small and medium-sized businesses, as they interact with other private-sector organizations, corresponding with the NIST guidance.

These capabilities should support swift communication among organizations, should enable coordination between the public and private sectors in multisector restoration efforts, and should aid in sharing mitigation strategies. DHS, the FBI, and DoD should affirm the applicability of, and where necessary further develop, existing safe harbor mechanisms to protect parties exchanging interdependency information both with the government and

between organizations using government-supplied platforms. SSAs, the FBI, NIST, and the Small Business Administration (SBA) should coordinate their efforts and ensure that industry and others are fully aware of the value, use, and applicability of the interdependency toolkit and associated standards of performance.

Action Item 1.2.5: *With the increase in wireless network communications across all organizations, and the nation's growing reliance on the Global Positioning System (GPS) to provide positioning, navigation, and timing (PNT), cybersecurity strategies must specifically address the full range of risks across the electromagnetic spectrum. An immediate goal should be enhancing the nation's ability to detect and resolve purposeful wireless disruptions and to improve the resilience and reliability of wireless communications and PNT data.* (SHORT TERM)

Specifically, the President should create a national, cross-government, public-private initiative to detect, collect, centralize, analyze, and respond to disruptions of wireless communications. This initiative should be coordinated with the multiagency, National Security Council (NSC)-chartered, DoD-led Purposeful Interference Response Team. In furtherance of this goal, there should be a national effort to train and equip federal law enforcement agents and, where appropriate, state and local police to rapidly identify, locate, and respond to wireless disruptions.

In addition, the President and Congress should prioritize national efforts to ensure the continued availability, reliability, redundancy, and overall resiliency of GPS signaling data. These efforts should include developing contingency plans for GPS/PNT systems and conducting tabletop exercises of those plans to ensure that relevant federal and SLTT organizations understand their roles in contingency and failover (switching equipment to standby when the main system fails).

Recommendation 1.3: The next Administration should launch a national public-private initiative to achieve major security and privacy improvements by increasing the use of strong authentication to improve identity management.

Strong identity management is key to much of what we do in the digital economy. In 2004, an industry leader predicted the demise of the traditional password because it cannot "meet the

challenge” of keeping critical information secure.¹¹ His analysis was right; yet we still rely on username and password as the most common form of identification and authentication. In doing so, we are making it far too easy for malicious actors to steal identities or impersonate someone online. However, a variety of factors inhibit the commercial adoption of large-scale identity management frameworks that offer stronger and more usable authentication, including convenience and the lack of uniform standards. Compounding these challenges is the need for identity solutions for connected devices.

A review of the major breaches over the past six years reveals that compromised identity characteristics have consistently been the main point of entry.¹² An ambitious but important goal for the next Administration should be to see no major breaches by 2021 in which identity—especially the use of passwords—is the primary vector of attack. Achieving this goal will enhance consumer trust in online transactions, but it will require identity solutions that are secure, privacy-enhancing, efficient, usable, and interoperable. Ultimately, these solutions need to be easy to use by individuals who are accessing digital devices and networks; otherwise identity management will remain a vector for attack. This approach requires a fundamental shift in thinking on the part of designers and those responsible for cybersecurity toward making authentication stronger and simple to use.

An effective identity management system is foundational to managing privacy interests and relates directly to security. Individuals should not have to be concerned about whether their personal information or information about their behaviors will be tracked without their direct involvement and consent. They should be comfortable knowing that the transmission of information to support identification in an online transaction will be minimized and will not include unnecessary data. Good privacy policies can enhance cybersecurity by accurately representing the ways in which the systems they govern actually operate. A privacy impact assessment that identifies and mitigates potential risks is another important tool for organizations as they carefully consider the information being collected, retained, and stored.

A good start to effective identity management has been initiated through the National Strategy for Trusted Identities in Cyberspace (NSTIC). NSTIC was instituted five years ago as a collaborative effort between the private and public sectors to create an identity ecosystem and establish a framework of overarching interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms. The Commission believes that NSTIC’s vision aptly summarizes the identity management of the future: “Individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation.”¹³ Pilot projects funded by NSTIC have resulted in a variety of strong authentication solutions in applications ranging from health care, finance, education, and retail to aerospace and government. NSTIC-generated identity solutions have been innovative and proven in real-life settings, but they have not yet achieved broad transformation. Public- and private-sector adoption at greater scale is needed. The Commission believes that the effective partnership model fostered by NSTIC should continue to serve as the foundation for a strong and vibrant identity ecosystem: the action items below are designed to move us toward this goal.

Other important work that must be undertaken to overcome identity authentication challenges includes the development of open-source standards and specifications like those developed by the Fast IDentity Online (FIDO) Alliance. FIDO specifications are focused largely on the mobile smartphone platform to deliver multifactor authentication to the masses, all based on industry-standard public key cryptography. Windows 10 has deployed FIDO specifications (known as Windows Hello),¹⁴ and numerous financial institutions have adopted FIDO for consumer banking. Today, organizations complying with FIDO specifications are able to deliver secure authentication technology on a wide range of devices, including mobile phones, USB keys, and near-field communications (NFC) and Bluetooth low energy (BLE) devices and wearables. This work, other standards activities, and new tools that support continuous authentication provide a

11 Bill Gates, Chairman, Microsoft, RSA Security Conference, February 25, 2004.

12 Interview with Jeremy Grant, former Senior Executive Advisor for Identity Management, NIST, October 28, 2016, conducted by Kiersten Todt.

13 The White House, “National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy,” April 2011, p.2, https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

14 “What Is Windows Hello,” Microsoft.com, <https://support.microsoft.com/en-us/help/17215/windows-10-what-is-hello>.

strong foundation for opt-in identity management for the digital infrastructure.

Action Item 1.3.1: *The next Administration should require that all Internet-based federal government services provided directly to citizens require the use of appropriately strong authentication.* (SHORT TERM)

Identity management is a major cybersecurity issue for which government can be an effective catalyst for large-scale adoption. The federal government should adopt industry-based capabilities for strong authentication for all external-facing applications that require identity management. Coordinated efforts should immediately be initiated for a variety of external-facing government services, including for tax services at the Internal Revenue Service; for immigration, secure flight, and entry/exit at the Department of Homeland Security; for social security accounts at the Social Security Administration; for passport services at the Department of State; and for health care programs at the Centers for Medicare and Medicaid Services. The Commission believes strongly that if government requires strong authentication, the private sector will be more likely to do the same.

This approach has the added value of not only securing federal applications directed at citizens but also creating a broader identity ecosystem of solutions that deliver better security, privacy, trust, usability, choice, and convenience for both public- and private-sector applications. The most important action that government can take to catalyze private-sector adoption of the right kind of solutions for consumers is to use these solutions in its own citizen-facing applications. The private sector will follow the government's lead if the government sets a high bar—and clears it. Specifically, private-sector organizations, including top online retailers, large health insurers, social media companies, and major financial institutions, should use strong authentication solutions as the default for major online applications.

Action Item 1.3.2: *The next Administration should direct that all federal agencies require the use of strong authentication by their employees, contractors, and others using federal systems.* (SHORT TERM)

The next Administration should provide agencies with updated policies and guidance that continue to focus on increased adoption of strong authentication solutions, including but, importantly, not limited to personal identity verification (PIV) credentials. To ensure adoption of strong, secure authentication

by federal agencies, the requirements should be made performance based (i.e., strong) so they include other (i.e., non-PIV) forms of authentication, and should mandate 100 percent adoption within a year.

Action Item 1.3.3: *The government should serve as a source to validate identity attributes to address online identity challenges.* (MEDIUM TERM)

The next Administration should create an interagency task force directed to find secure, user-friendly, privacy-centric ways in which agencies can serve as one authoritative source to validate identity attributes in the broader identity market. This action would enable government agencies and the private sector to drive significant risk out of new account openings and other high-risk, high-value online services, and it would help all citizens more easily and securely engage in transactions online.

As part of this effort, the interagency task force should be directed to incentivize states to participate. States—by issuing drivers' licenses, birth certificates, and other identity documents—are already playing a vital role in the identity ecosystem; notably, they provide the most widely used source of identity proofing for individuals. Collaboration is key. Industry and government each have much to gain from strengthened online identity proofing. The federal government should support and augment existing private-sector efforts by working with industry to set out rules of the road, identify sources of attributes controlled by industry, and establish parameters and trust models for validating and using those industry attributes.

Action Item 1.3.4: *The next Administration should convene a body of experts from the private and public sectors to develop identity management requirements for devices and processes in support of specifying the sources of data.* (SHORT TERM)

The Internet of Things is causing massive data proliferation through devices that are capturing, aggregating, and processing data. We are at the early stages of using this data to make choices that affect all aspects of our lives, from personal decisions to decisions that affect the nation. Trust in those decisions requires confidence in the devices that captured, aggregated, and processed the data, as well as assurance that the data have not been accidentally or maliciously altered. This trust will come from being able to identify devices that act on their own, like sensors, or devices that are associated with a person, like a mobile phone. Today, few devices can be

uniquely identified, and data flows between devices are not well understood. We therefore must consider the problem of identity management from the perspective of being able to securely and efficiently identify not just people, but also individual devices and the data that come from them.

Recommendation 1.4: The next Administration should build on the success of the Cybersecurity Framework to reduce risk, both within and outside of critical infrastructure, by actively working to sustain and increase use of the Framework.

Organizations need to make informed, smart choices about risks to their assets and operations and to set priorities for cybersecurity efforts and investments—just as they do in dealing with other enterprise risks. The *Framework for Improving Critical Infrastructure Cybersecurity*, more widely known as the Cybersecurity Framework, was called for by Executive Order 13636 in January 2013 and released in February 2014.¹⁵ The development of this voluntary framework was coordinated by NIST through a collaborative process involving industry, academia, and government agencies.

The Framework provides a risk-based approach for cybersecurity through five core functions: identify, protect, detect, respond, and recover. It is designed to assist organizations of any size, in any sector, and at any stage of their cybersecurity maturity. The Framework provides a vocabulary to bridge the communication gap that sometimes exists between technologists and executives. NIST was directed to create the Framework specifically for managing cybersecurity risks related to critical infrastructure, but a broad array of private- and public-sector organizations across the United States—and some around the world—now use it. There is potential for even more widespread use of the Framework's risk management approach to address and reduce cybersecurity issues.

The Cybersecurity Framework is playing an important role strengthening the risk management ecosystem, and if effectively implemented it can reduce the need for future legislation and regulation. For this reason, the Commission recommends focusing additional attention on cybersecurity risk measurement and conformity assessment. Risk management and measurement can

be helpful in making decisions about cyber insurance coverage and possibly in reducing premiums.

The Framework has tremendous value for organizations (such as small businesses and state, local, tribal, and territorial governments) that are resource constrained and need an efficient and effective way to address cybersecurity risk. In addition, the Cybersecurity Framework augments existing Federal Information Security Modernization Act (FISMA) practices used by federal agencies. The Framework already has proven its value to larger organizations, both up and down the management chains from boards of directors and chief executives to the IT and business operations. In short, the Framework is a low-cost, high-yield option for enhancing cybersecurity.

The Commission heard repeatedly in workshops, from stakeholders, and in public comments that the Cybersecurity Framework is a highly valued tool for managing cyber risk. Still, many organizations, including the majority of federal and other government agencies, are not yet taking advantage of it. The Commission believes that the Framework should be better utilized, both domestically and globally, by all organizations inside and outside government for greater impact.

The Commission recommends the publication of information, including example and sector profiles, to help smaller companies use the Cybersecurity Framework. The Commission emphasizes the importance of ensuring continuous updates to the action items below to align with evolving capabilities.

Action Item 1.4.1: *NIST, in coordination with the NCP³, should establish a Cybersecurity Framework Metrics Working Group (CFMWG) to develop industry-led, consensus-based metrics that may be used by (1) industry to voluntarily assess relative corporate risk, (2) the Department of Treasury and insurers to understand insurance coverage needs and standardize premiums, and (3) DHS to implement a nationwide voluntary incident reporting program for identifying cybersecurity gaps. This reporting program should include a cyber incident data and analysis repository (CIDAR).*
(SHORT TERM)

The CFMWG would develop meaningful metrics for better understanding and quantifying the benefits that use of the Framework brings to organizations that adopt it. Most current efforts to measure cybersecurity effectiveness focus on the actions taken by an organization, rather than on those actions'

¹⁵ <https://www.nist.gov/cyberframework>.

effectiveness. This group's work should help address that gap, offering quantifiable information that can be used to improve the Framework and more precisely demonstrate where and how its use is most effective.

The metrics developed must also be useful for insurers seeking to understand evolving coverage needs. The discrete risks associated with insurance coverage must be measurable, so that insurers can have a stronger basis for making coverage decisions and standardizing insurance premiums. Preexisting public-private collaborations such as the Department of Treasury-led Financial and Banking Information Infrastructure Committee (FBIIC) are logical venues to gather input for the CFMWG, share the resulting consensus metrics, and discuss the use of those metrics. It is important that the Working Group's approach to metrics be consistent and align with that of the cyber incident data and analysis repository (CIDAR). This repository will provide the insurance industry with metrics to be used in actuarial calculations and modeling and enable the industry to understand the sector differentiation of aggregate risks and effective practices. A CIDAR will also enable organizations of all types to better manage information security risks by helping them to understand peer-to-peer benchmarking and by supporting effective cost-benefit analysis. It will also highlight the returns on cybersecurity investments.

Voluntary incident reporting data will greatly inform the development of CFMWG's metrics. For this reason, it is important that Congress provide DHS with the resources to expand the current CIDAR pilot to a national capability via a grant program. Congress also needs to eliminate key barriers to private-sector participation in a CIDAR by providing protections to industry modeled on those granted by the 2015 Cybersecurity Information Sharing Act. DOJ and DHS can greatly bolster CIDAR incident reporting data by ensuring that all federal cyber incident reporting mechanisms—including those of the FBI, the United States Secret Service, and the Internet Crime Complaint Center (IC3)—request data to be submitted automatically to supplement the CIDAR's repository, consistent with federal privacy and security regulations.

Action Item 1.4.2: *All federal agencies should be required to use the Cybersecurity Framework.* (SHORT TERM)

Federal agencies now are encouraged, but not required, to use the Cybersecurity Framework. Notably, some are infusing the core functions of the Framework into the language of cybersecurity risk management efforts. Other agencies are using the Framework as an overarching guide to improve their management of risk and to set implementation priorities, pursuing the improvements that will have the greatest impact. However, many agencies are not yet using the Cybersecurity Framework. They may be reluctant to do so because they are focused on the many requirements that they face, or because they do not understand how they can make productive use of the Framework within the larger context of managing their operations. To address the lack of urgency displayed by the majority of agencies, the Office of Management and Budget (OMB) should mandate their use of the Framework as part of their enterprise risk management approach. (For additional details, see *Imperative 5, Recommendation 5.3.*) NIST should also provide agencies with additional guidance.

Using the Cybersecurity Framework would bring immediate benefits, driving agencies to shift their approaches away from simple compliance and toward thinking more holistically about cybersecurity risk management.

Action Item 1.4.3: *Regulatory agencies should harmonize existing and future regulations with the Cybersecurity Framework to focus on risk management—reducing industry's cost of complying with prescriptive or conflicting regulations that may not aid cybersecurity and may unintentionally discourage rather than incentivize innovation.* (SHORT TERM)

The private sector has voiced strong concerns about the ways in which regulatory agencies are beginning to use the Cybersecurity Framework—or in which they refer inconsistently to the Framework, as each agency makes different decisions about its application. Such disparate regulations risk redundancy and confusion among regulated parts of our economy. Federal regulators should harmonize their efforts relating to the Framework, an action called for in Executive Order 13636 but never executed. Regulatory agencies should make explicit how

their requirements map to the Cybersecurity Framework, as the Federal Trade Commission has done.¹⁶

OMB should also issue a circular that makes the adoption of regulations that depart significantly from the Cybersecurity Framework explicitly subject to its regulatory impact analysis, quantifying the expected costs and benefits of proposed regulations. Because of the efficiencies and reduced compliance costs that covered entities would realize from a common framework, an agency that advances an approach which substantially departs from the baseline framework would be required to make the case that its added cost is outweighed by a public benefit. Likewise, to reduce the impact on industry of overlapping and potentially conflicting requirements, it is important that state and local regulatory agencies strongly consider aligning their approaches with the risk management-oriented Cybersecurity Framework.

Action Item 1.4.4: *The private sector should develop conformity assessment programs that are effective and efficient, and that support the international trade and business activities of U.S. companies.* (SHORT TERM)

Conformity assessment is an approach by which organizations determine and demonstrate that they are exercising diligence with regard to cybersecurity. When an industry-driven approach is widely used, conformity can be a powerful tool to reduce industry risk—if the assessment regime promotes meaningful results and outcomes, rather than simply affirming that a review has been conducted. Organizations want to have confidence that they, their business partners and collaborators, and their supply chain are effectively managing risk. They also wish to demonstrate their conformance in order to bolster trustworthy business relationships. In this respect, conformance is a helpful tool for organizations seeking to expand partnerships and other business relationships.

Conformity assessments conducted by private-sector organizations can increase productivity and efficiency in government and industry, expand opportunities for international trade, conserve resources, improve health and safety, and protect the environment.

The increasing use of the Cybersecurity Framework, both in critical infrastructure and beyond, makes it a good basis for conformity assessment. The conformity assessment that is being undertaken by the private sector could, in part, meet the needs of owners and operators, business partners, and supply chains in demonstrating their effective use of the Cybersecurity Framework.

Action Item 1.4.5: *The government should extend additional incentives to companies that have implemented cyber risk management principles and demonstrate collaborative engagement.* (SHORT TERM)

Incentives must play a more substantial role in building a cyber-secure nation. To accomplish this goal, the next Administration and Congress should pass legislation that provides appropriate liability protections for businesses that engage in cyber risk mitigation practices that are consistent either with the Cybersecurity Framework or with common industry segment practices, and that engage in cyber collaboration with government and industry. Safe harbors would be particularly appropriate to consider in the context of providing business certainty for companies that operate in regulated sectors. Additional benefits to encourage enhanced cybersecurity might include tax incentives, government procurement incentives, public recognition programs, prioritized cyber technical assistance, and regulatory streamlining. In addition, research and development efforts should specifically include a detailed study of how best to improve network security through incentives.

Recommendation 1.5: The next Administration should develop concrete efforts to support and strengthen the cybersecurity of small and medium-sized businesses (SMBs).

There are more than 28 million small businesses in the United States. These businesses produce approximately 46 percent of our nation's private-sector output and create 63 percent of all new jobs in the country.¹⁷ Nearly all rely on information technologies, including the Internet, other digital networks, and a variety of devices. For some small businesses, the security of their information, systems, and networks either is not their highest priority or is something they do not have the resources to address. A cybersecurity incident can harm their business,

16 Andrea Arias, "The NIST Cybersecurity Framework and the FTC," August 31, 2016, <https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc>.

17 U.S. Small Business Administration, Office of Advocacy, "Frequently Asked Questions," March 2014, p.1, https://www.sba.gov/sites/default/files/FAQ_March_2014_0.pdf.

customers, employees, and business partners. Incidents involving their companies can also have far broader consequences, adversely affecting segments of the digital economy. The federal government can and should provide assistance to these companies.

Action Item 1.5.1: *The National Institute of Standards and Technology (NIST) should expand its support of SMBs in using the Cybersecurity Framework and should assess its cost-effectiveness specifically for SMBs. (SHORT TERM)*

The Cybersecurity Framework is being adopted by organizations of all sizes, but many smaller businesses are unclear about how to use it. NIST recently published “Small Business Information Security: The Fundamentals”¹⁸ based in part on the Framework. NIST should continue to help SMBs use the Cybersecurity Framework, and expand those efforts. That help should take the form of implementation-ready “profiles” that address commonly occurring business objectives (e.g., availability of Web services, confidentiality of intellectual property) using the Cybersecurity Framework. These Framework profiles should align an organization’s cybersecurity activities with its business requirements, risk tolerance, and resources, and should aid in the communication of risk within and between organizations. NIST, DHS, the SBA, and SSAs should educate SMBs on the use of the profiles in achieving desired business outcomes. This outreach should be included as part of these agencies’ ongoing cybersecurity information and assistance programs. Significantly, NIST should provide fact-based metrics to establish whether and to what extent use of the Framework is effective.

Action Item 1.5.2: *DHS and NIST, through the National Cybersecurity Center of Excellence (NCCoE), in collaboration with the private sector, should develop blueprints for how to integrate and use existing cybersecurity technologies, with a focus on meeting the needs of SMBs. (SHORT TERM)*

The federal government develops best practice guides for cybersecurity and it provides technical assistance to smaller businesses. It is not currently providing customized guidance about how to integrate and use cybersecurity technologies that are available to meet a variety of needs that small businesses face. DHS and NIST, through the NCCoE, should initiate focused

efforts—including the use of private-sector partners and collaborators—to provide the kind of practical guides needed by small and medium-sized companies that have limited technical capabilities, time, and resources. These guides should be consistent with the Cybersecurity Framework.

Action Item 1.5.3: *Sector-specific agencies (SSAs) and industry associations and organizations should collaborate to develop a program to review past public cyber attacks to identify lessons learned from the event, including a focus on application to SMBs. (SHORT TERM)*

Government and the private sector should collaborate to develop this program, which would translate lessons learned into guidance to mitigate the vulnerabilities exploited. This guidance should be tailored for SMBs.

18 <http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>.

Imperative 2: Innovate and Accelerate Investment for the Security and Growth of Digital Networks and the Digital Economy

The Challenge and Way Forward

The “Internet of Things” (IoT) is a buzz phrase that is associated with a great deal of marketing hype, and as such was a term mostly ignored by policy makers and the public until about a year ago. In the digital world, “the future” arrives quickly, and the core technical idea behind the IoT—a proliferation of devices ranging from ordinary household appliances and toys to industrial process controllers, all connected to the Internet—is leading the way. Within the past several years, the complex and expanding information technology network that was dominated by the Internet has become much more connected with the physical world. It is increasingly difficult to identify equipment or devices that are not, or could not be, connected to the Internet to provide improved capabilities in health care, transportation, retail, and other sectors of our economy and society. We are experiencing a revolution in which all objects in our daily lives are converging on similar computing and communication capabilities, and therefore also on similar susceptibility to cyber threats.

Because this convergence causes the “things” in our lives to become infused with information technology and linked with worldwide connections, IoT users become meaningful participants in the nation’s cybersecurity. The IoT blurs the distinctions between critical infrastructure, regulated devices, and consumer products. The less aware consumers are of this connectivity and its security implications, the more likely it is that personal devices—even devices as ordinary as coffeemakers and thermostats—could be compromised by malicious actors.

Connected devices—which include both cyber physical IoT devices that interact with the physical world and other information technologies, such as smartphones and personal computers—are so ubiquitous that segregating them from networks that host critical infrastructure devices or other operational technology (OT)—managed devices may soon become completely impractical. The consequences for cybersecurity are enormous, as we are just beginning to experience. In September 2016, the largest distributed denial-of-service (DDoS) attack ever recorded—almost twice as powerful as any before—was

orchestrated using a botnet that relied on compromised IoT devices.¹⁹ Another attack took place the following month. Purely personal or consumer technology can be used, maliciously, at large scale with highly detrimental impacts. Indeed, as the attacks in recent months make clear, IoT devices can be significant weak links in our global networks, easily weaponized to deliver destructive and destabilizing attacks. And while the attacks we are witnessing today may appear to be limited mainly to DDoS, as the computing power in connected devices increases—and as we come to depend on them to control, either directly or indirectly, machinery with the power to create kinetic effects (whether electrical or mechanical)—the dangers will increase dramatically.

We must improve the standards, guidelines, and best practices available to secure these connected devices and systems. Of course, these are effective only if they take hold and become part of the supply chain. It is essential that companies selling connected devices ensure that their suppliers require the same security in components and subcomponents, and that they take steps via the testing process to enforce those requirements.

To understand the cybersecurity implications of the widespread deployment of connected devices, the public will need to be better educated and more involved. The goal should be to achieve security by default in all connected devices and to ensure that the consumer and integrator alike know what security capabilities are, or are not, contained in these devices.

The IoT is an area of special concern in which fundamental research and development (R&D) is needed not just to develop solutions that continue to foster innovation, but also to build in opportunities for reducing the risk involved with ubiquitous connectivity. In the United States, the private sector generally funds and focuses on near-term research and on transitioning successful research (from any source) into commercial products. Government funding of long-term, high-risk research and of

19 Igal Zeifman, Dima Bekerman, and Ben Herzberg, “Breaking Down Mirai: An IoT DDoS Botnet Analysis,” October 26, 2016, <https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html>.

mission-specific R&D thus remains critically important. Despite the large overall investment in cybersecurity R&D, funding for creating inherently secure technology, products, systems, and environments is in comparison relatively small. The government should invest in fundamental cyber R&D that will foster the development of inherently secure, defensible, and resilient/recoverable systems. The private sector should help determine this research agenda and work with federal agencies to ensure that the results of this research are readily usable in improving technologies, products, and services.

Recommendation 2.1: The federal government and private-sector partners must join forces rapidly and purposefully to improve the security of the Internet of Things (IoT).

The term “IoT” describes everything from jet engines to children’s toys to industrial machinery. For example: a pocket step counter and an implanted pacemaker are both small, battery-powered health devices that sense body functions, can connect to networks, and take actions accordingly. Both are squarely within the IoT. Yet one is life-critical while the other is a disposable consumer good—and the two are almost entirely distinct in the considerations of design, security, and operation that went into creating them.

The IoT is collapsing our concepts of individual sectors, businesses, and architectures by its ubiquitous connectivity and use of other powerful capabilities such as network protocols and cloud computing. This technological development is forcing us to reconsider our definitions of sectors, perimeters, trust, and control.

One main concern in assessing the security needs of an IoT device should be where and how it can be used: a pacemaker needs to be designed to exact specifications, while a consumer-grade fitness tracker can be designed to a different set of security standards. We need both a set of general security principles specified in international standards and IoT recommendations tailored to specific sectors, applications, and risks.

The United States must lead a global push to drive security and secure development concepts into IoT design and development. The hour for doing so is already late. The first generations of IoT devices—billions in number—have already been deployed in homes, hospitals, and automobiles across the nation. Some devices are secure but most are not, as seen in recent attacks and in malware that exploits poor security designs, deployments, and

configurations in devices. Weak security carries enormous safety implications. Moreover, privacy protections are frequently an afterthought in the design of these devices.

Some observers argue that the window for securing IoT devices has closed, but the Commission believes that an opportunity to make the standard “secure to market” still exists, particularly in the production of single-purpose life-critical or safety items for consumers. (Consumer labels and rating systems are discussed further in *Imperative 3, Action Item 3.1.1.*) The private sector and government must partner in this effort, as they already are doing in some areas, including the development of self-driving cars. Where IoT is deployed in life-critical environments, designers and manufacturers need to closely examine the balance between efficiency and security to ensure that security is not compromised in life-threatening ways for the sake of innovation. Driving security requirements away from the end user, particularly for consumer-facing IoT connected devices, is critical.

Agencies that currently regulate IoT devices should follow the example of the National Highway Traffic Safety Administration (NHTSA) and begin working immediately with industry to develop voluntary and collaborative guidelines to secure IoT devices. For example, automotive manufacturers have called for a consistent set of federal guidelines for autonomous vehicles, and they have worked with the NHTSA on such rules.²⁰

Action Item 2.1.1: *To facilitate the development of secure IoT devices and systems, within 60 days the President should issue an executive order directing NIST to work with industry and voluntary standards organizations to identify existing standards, best practices, and gaps for deployments ranging from critical systems to consumer/commercial uses—and to jointly and rapidly agree on a comprehensive set of risk-based security standards, developing new standards where necessary. (SHORT TERM)*

These risk-based security standards should be scalable and tailored to the direct impacts of a device or system being compromised, while still achieving a common baseline level of security.

20 U.S. Department of Transportation, NHTSA, “Federal Automated Vehicle Policy: Accelerating the Next Revolution in Roadway Safety,” September 2016, <http://www.nhtsa.gov/nhtsa/av/index.html>.

Of course, these security standards alone will not benefit the public unless consumers are able to readily assess whether the devices they purchase comply with them. Yet consumers cannot be expected to understand the technical details of the variety of connected devices they use. To bridge this information gap, nongovernmental organizations, on the model of UL or Consumer Reports, should develop clear and understandable labels to assist consumers in understanding the cybersecurity risks of the products they purchase. These labels should be based, at least in part, on whether and to what degree a given device conforms to the standards and best practices that NIST identifies. (Consumer labels and rating systems are discussed further in *Imperative 3, Action Item 3.1.1.*) Together, standards and conformity assessments can positively impact almost every aspect of the IoT.

The federal government's procurement processes may also be used to incentivize conformity with these standards, by making conformance an explicit component of vendor bids or product selection.

Action Item 2.1.2: *Regulatory agencies should assess whether effective cybersecurity practices and technologies that are identified by the standards process in Action Item 2.1.1 are being effectively and promptly implemented to improve cybersecurity and should initiate any appropriate rule making to address the gaps.* (MEDIUM TERM)

Because devices that use common computing platforms and span multiple markets, areas, and infrastructures are proliferating, federal regulatory agencies should start any new regulatory action using a standards-based approach. They should cite items identified and developed in Action Item 2.1.1 where practical, and in accordance with OMB guidance,²¹ as well as undertaking public-private partnerships.

The NIST-led process should include the active participation of appropriate federal and state regulatory bodies to facilitate their efforts. OMB's Office of Information and Regulatory Affairs (OIRA), in coordination with federal standards officials as defined in OMB Circular A-119, should monitor and assess the state of

IoT and connected device cybersecurity and report on progress and gaps on a regular basis. If additional gaps are identified that regulation is unable to address, OMB should work with Congress to propose appropriate action.

Action Item 2.1.3: *The Department of Justice should lead an interagency study with the Departments of Commerce and Homeland Security and work with the Federal Trade Commission, the Consumer Product Safety Commission, and interested private-sector parties to assess the current state of the law with regard to liability for harm caused by faulty IoT devices and provide recommendations within 180 days.* (SHORT TERM)

To the extent that the law does not provide appropriate incentives for companies to design security into their products, and does not offer protections for those that do, the President should draw on these recommendations to present Congress with a legislative proposal to address identified gaps, as well as explore actions that could be accomplished through executive order.

Action Item 2.1.4: *The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) should develop and communicate guidelines for IoT cybersecurity and privacy best practices for rapid deployment and use.* (SHORT TERM)

Initial best practices should include requirements to mandate that IoT devices be rendered unusable until users first change default usernames and passwords. Weak usernames and passwords would be rejected by the device. ICS-CERT, DHS, and NIST should work with industry and fund grants to develop secure open-source software that is purpose-built to support certain types of IoT devices over the full life cycle of each product.

Recommendation 2.2: The federal government should make the development of usable, affordable, inherently secure, defensible, and resilient/recoverable systems its top priority for cybersecurity research and development (R&D) as a part of the overall R&D agenda.

The Commission recommends that federal R&D funding for cybersecurity increase by approximately \$4 billion over the next 10 years for the federal civilian agencies,²² with a high priority

21 Office of Management and Budget, Executive Office of the President, revision of OMB Circular No. A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities," January 27, 2016, https://www.whitehouse.gov/sites/default/files/omb/inforeg/revise_circular_a-119_as_of_1_22.pdf.

22 Funding increase based on current cybersecurity R&D funding reported in FY 17 NITRD President's Budget Request to move from \$714 million per year to \$900 million to \$1.2 billion per year.

given to efforts that will result in the use, integration, and deployment of affordable, inherently secure, privacy-protecting, usable, functional, resilient, recoverable, and defensible systems.

Current efforts in cybersecurity R&D are not as well coordinated and balanced as they should be. Many resources, in terms of time, talent, and funding, are being used to develop additional reactive capabilities that identify threats and vulnerabilities, provide some additional protection, detect threat activity, and respond to threat actions. We will be unable to shift the advantage in cyberspace away from attackers until we collectively recognize that continued dependence on reactive cybersecurity makes it easier for attackers to find compromised systems: our R&D priorities should be rebalanced to address this need and to maximize impact.

Far too few resources are being devoted to creating inherently secure technology products, systems, and environments or to understanding how existing technology supporting this goal can best be adopted and integrated. Dramatic increases are needed in the cybersecurity capabilities in the systems on which we rely (particularly in the civilian commercial sector) as well as the technology products and services that those systems use. Such a significant increase can be accomplished only through a national R&D effort targeted at creating defensible systems that are usable, secure, and resilient. These systems should be designed, built, deployed, and configured in such a way that they are inherently secure, protect privacy, degrade gracefully, and support simple and fast recovery when compromises occur while still maintaining functionality and supporting business needs and missions.

An inherently secure system would be unassailable: that is, it would be a system for which significant vulnerabilities either provably do not exist or are exceptionally hard to find and exploit without quick detection and remediation. The best approach to achieving such systems entails interweaving development practices, using computationally hard protections, conducting empirical analysis throughout the system's development life cycle, and implementing system components in ways that are verifiable, accountable, and adaptable.

Private investment in products and services tends to undervalue cybersecurity, as the urge to be "first to market" too often

outweighs the need to be "secure to market." In addition to rebalancing and increasing funding for work on more inherently secure technologies, the federal government should direct more attention to cybersecurity-related research outside of traditional technical areas.

Support should be provided for cybersecurity R&D focused on human factors and usability, public policy, law, metrics, and the societal impacts of cybersecurity. Advances in these areas are critical to ensuring the successful adoption and use of both existing technologies and those that are being developed. This research would especially assist in meeting the cybersecurity needs of users—particularly individuals and small and medium-sized businesses.

Action Item 2.2.1: *The Director of the Office of Science and Technology Policy (OSTP) should lead the development of an integrated government–private-sector cybersecurity roadmap for developing usable, affordable, inherently secure, resilient/recoverable, privacy-protecting, functional, and defensible systems. This effort should be backed by a significant R&D funding increase in the President's Budget Request for agencies supporting this roadmap. (SHORT TERM)*

Today's systems are not resilient against serious attacks: that is, they are not inherently secure and defending them is difficult—and, in some cases, not even possible. Software for these systems has been developed using software components, programming languages, and testing methods and other practices that do not appropriately take security into account. Although the current scope of cybersecurity R&D includes enabling the creation of resilient systems, this work must be broadened and its time frame accelerated. In the past, defensible systems were difficult to use, did not support the workflow of businesses, and consequently were not employed. Markets, users, and society more generally did not understand or appreciate such systems. While current products exist that support this goal of inherent security, they are not sufficiently integrated into U.S. government systems or the devices and network in our national economy. Focused research is needed to address this issue.

Making secure systems and devices the norm requires more thoughtful and coordinated R&D planning to set goals for the next

decade; it also requires increases in R&D funding for researchers in government, industry, and academia so that those goals can be met. The Federal Cybersecurity Research and Development Strategic Plan released in February 2016²³ includes several federal R&D objectives that support the creation of more resilient software. These should be built on and expanded.

In conducting this research, greater use should be made of challenge competitions—with money prizes—and other creative approaches that engage individuals and teams of innovators. These competitions should include development of new technologies, along with innovation in the use and systems integration of existing inherently secure technologies. The cybersecurity community has had some success with the challenge competition model, especially the Cyber Grand Challenge created recently by the Defense Advanced Research Projects Agency (DARPA). These efforts should be sustained, multiyear, and iterative. Examples of possible challenge competition topics include privacy-enhancing technologies, IoT security, defect-free software, blockchain, and pervasive encryption.

Action Item 2.2.2: *The U.S. government should support cybersecurity-focused research into traditionally underfunded areas, including human factors and usability, policy, law, metrics, and the social impacts of privacy and security technologies, as well as issues specific to small and medium-sized businesses where research can provide practical solutions. (SHORT TERM)*

The federal civilian and defense R&D agencies should support academia, industry, and research foundations conducting research that supports the OSTP-led plans. This support should also include cybersecurity policy research. A useful complement to (but not substitute for) such federal investment would be support from private-sector entities, such as foundations.

23 National Science and Technology Council, Networking and Information Technology Research and Development Program, “Federal Cybersecurity Research and Development Strategic Plan: Ensuring Prosperity and National Security,” Executive Office of the President of the United States, February 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf.

This page intentionally left blank.

Imperative 3: Prepare Consumers to Thrive in a Digital Age

The Challenge and Way Forward

Innovation in computing technologies continues to accelerate. While this innovation enables exciting new capabilities every day, it is happening in a way that often places the burden on individuals to understand if a product or service is secure to use and to take actions to secure their devices and their use of those devices. Moreover, consumers often are unaware that buying and using secure devices does more than mitigate threats to their own devices and data: their responsible cyber habits also strengthen and protect the broader networks of all users who rely on the Internet and the digital ecosystem.

Engineers and designers should create products and systems with security built in and provide consumers with the ability to know how their user experience will be protected. The burden of primary responsibility for cybersecurity should be driven up the chain from the consumer to the manufacturer. The Commission believes that this goal must be met in order to enhance cybersecurity, especially as IoT devices rapidly enter the consumer world. These shifts must be accompanied by much-improved identity management approaches that include stronger authentication. (See *Imperative 1, Recommendation 1.3*.)

As an interim step to advance products designed with security built in, engineers and manufacturers should pursue “security awareness by default”—actively prompting consumers to change default passwords, select security preferences, and verify that they are aware of the security implications of an action, for example.

The complexity of cybersecurity and the resources needed to address it must be reduced. In the long run, manufacturers should automate, simplify, and improve the process by which consumers are advised about the cybersecurity implications of using their digital devices. They must come up with more intuitive ways that demand the minimum amount of extra thought and effort.

Recommendation 3.1: Business leaders in the information technology and communications sectors need to work with consumer organizations and the Federal Trade Commission (FTC) to provide consumers with better information so that

they can make informed decisions when purchasing and using connected products and services.

Despite near-universal dependence on computing technology and information exchange for communication, education, commerce, transportation, housing, health care, and many other aspects of daily life, most consumers are unsure about how to protect their data and personal information, much less select the technology products and services that best support their cybersecurity and privacy needs.

Raising cybersecurity awareness has long been a core aim of U.S. cybersecurity strategy, and the notion that consumer awareness about cybersecurity should be heightened is broadly accepted. Yet public- and private-sector efforts have fallen far short of achieving this goal. The Commission identified many previous and current federal, private-sector, and nonprofit attempts to increase cybersecurity awareness for every demographic group, but these attempts have not produced the intended results. Unfortunately, some public awareness campaigns are carried out by organizations centered on technology, rather than by those whose expertise lies in public messaging and effecting behavioral change. These campaigns tend to be fitful, periodically highlighting cybersecurity instead of providing a constant focus on the topic. Narrowly framed, once-in-a-while approaches cannot sufficiently motivate people to change their cybersecurity behavior, and cannot achieve wide-scale, large-impact success in bolstering security in the larger digital economy. A sustained multidisciplinary public awareness campaign—focused on providing simple, concrete, actionable advice that consumers can and will follow—is needed. There are numerous public service campaigns that have achieved behavior-changing results across broad portions of the public; none has tackled as complex an issue as cybersecurity.

Increasing awareness is only part of the solution. To achieve the necessary behavioral change, such a campaign must be coupled with an improvement in the security incorporated into devices and systems. The ultimate solution is that all devices should be “secure to market.” But until then companies must provide information about each product sufficient to enable consumers to make informed and smart security-related decisions about the

technology products and services they acquire. Such disclosures should incentivize technology product vendors and service providers to give consumers clear, accurate, and comprehensive information about their cybersecurity and privacy capabilities and practices. A partial goal of this effort should be to make cybersecurity a market differentiator.

Action Item 3.1.1: *To improve consumers' purchasing decisions, an independent organization should develop the equivalent of a cybersecurity "nutritional label" for technology products and services—ideally linked to a rating system of understandable, impartial, third-party assessment that consumers will intuitively trust and understand. (SHORT AND MEDIUM TERM)*

Whether at their jobs or in their activities outside of work, consumers rely heavily on technology products and services in their daily lives. Today, there is no standard format in which technology companies communicate the security characteristics and features of their products to consumers. And for these products and services, unlike mainstream products that are subject to authoritative ratings based on standards and tests by well-known independent organizations, there is no system to let consumers know how they rate. This lack of information leaves most consumers unaware of the risks associated with using technology products and services, how these risks might easily be reduced, or how competing products' security characteristics compare with each other. Making matters worse, security considerations increasingly may lead to safety concerns, as many Internet-enabled devices can affect the world physically.

Though this is a complex challenge, improvements in consumer awareness and engagement can be made now. First, a standard cybersecurity label for technology products and services should be developed. This label should include privacy-related information and be informed by the Cybersecurity Framework. It should capture cybersecurity-related risks for a particular product or service, be user-friendly, and convey how easy the technology is for the consumer to secure properly. Each label should display reliable, quantifiable information for a technology product in a format easily understood by the product's consumers. Properly designed and deployed, a standard label would enhance consumer decision making.

Other areas of consumer information and purchase offer ample precedent for initiatives by one or more independent organizations that would lead to helpful labels. For example, such an effort could be modeled on the nutritional label mandated by the Food

and Drug Administration for food products, the Energy Star program and associated rating information for products that consume energy, labeling programs that use a sticker to provide standard information to prospective buyers of new vehicles, or consumer product–rating systems.

Second, a rating system based on an impartial assessment of a product's cybersecurity risk could be incorporated into the label or provided in associated literature as a further guide to consumers. Again, several models exist that could be expanded, amplified, or modified.

Labeling and rating systems will be far more challenging to advance for technology products, and likely will proceed in steps and evolve. Given the degree of difficulty involved, designing and launching a rating system will take the concerted efforts of multiple organizations in the private and public sectors—but the need merits a full-scale initiative. Private- and public-sector resources should be marshaled to tackle this task. A decision about whether such efforts should remain strictly voluntary should be made after initial efforts have had time to mature; later assessment may determine that a mandatory labeling or rating program is required. In the meantime, better information for consumers through public awareness campaigns, checklists, consumer-oriented websites, and formal education should receive urgent attention. This issue should be a top item on the agenda for the White House summit recommended below.

Action Item 3.1.2: *Within the first 100 days of the new Administration, the White House should convene a summit of business, education, consumer, and government leaders at all levels to plan for the launch of a new national cybersecurity awareness and engagement campaign. (SHORT TERM)*

There have been many public and private cybersecurity awareness campaigns during the past few years that have not achieved the anticipated results. Future awareness campaigns should build on these efforts and the knowledge gained about what approaches work most effectively. New initiatives should be undertaken at an even more ambitious scale aimed at reaching a larger audience and delivering a small number of clear and consistent messages on specific cybersecurity issues more frequently and across a wider variety of communications channels.

Campaigns can have greater impact if they are informed by the experiences of awareness campaigns in domains other than cybersecurity. Designing successful cybersecurity awareness

campaigns should involve gathering input from a wide range of viewpoints by drawing on experts from traditional and novel online media and content providers, advertisers, technology developers, public health experts, Internet service providers, and law enforcement, as well as business, education, consumer, and government leaders.

To gain the attention and resources that this effort deserves, the President should convene a summit that brings together experts, as soon as possible, to facilitate the launch of a new national cybersecurity awareness campaign in 2017. Among the topics that should be addressed at such a summit are the steps needed to launch initiatives designed to generate product and service labeling and rating systems.

In addition, specific attention should be given to the need to educate consumers on the selection and use of secure, connected IoT devices. This effort must include the importance of changing default usernames and passwords on their connected devices (routers, cameras, printers, etc.). The goal of this effort is twofold: (1) to improve security of the millions of IoT devices deployed currently and likely to be purchased in the future, and (2) to close off a vector commonly used in cyber attacks. The aim must be to minimize—though not entirely eliminate—the need for consumers to be responsible for IoT device security. The Federal Trade Commission (FTC) should use this summit to initiate work with IoT device manufacturers and usability experts to create websites, hotlines, and other approaches to assist consumers in changing default usernames and passwords. The FTC also should use this forum to gather consumer and industry representatives to better inform consumers about their rights and responsibilities pertaining to digital devices (see the following action item).

Action Item 3.1.3: *The FTC should convene consumer organizations and industry stakeholders in an initiative to develop a standard template for documents that inform consumers of their cybersecurity roles and responsibilities as citizens in the digital economy—along with a “Consumer’s Bill of Rights and Responsibilities for the Digital Age.” (MEDIUM TERM)*

Security and privacy of digital products or services depend on all ecosystem participants understanding their roles and responsibilities, and the consequences of their actions. Clarifying these expectations enables buyers to understand true costs and to differentiate among market alternatives. A single digital-

oriented consumer “bill of rights” could serve as a framework for all parties, including manufacturers, service providers, and consumers.

Consumers often do not know or understand what rights they may have regarding cybersecurity and privacy because there is no standard, and because current disclosures, if they exist, vary by product, service, and manufacturer. Providers of technology products and services usually express information about their consumer cybersecurity and privacy practices using legal language that most consumers cannot understand. Even if the explanations of these practices were written more accessibly, consumers would still have to take time to review the practices for each technology product and service; realistically, few if any would do so.

A document based on a standard template to educate consumers on their rights would make them much more knowledgeable about what security measures their products and services employ and what technology vendors and providers are legally allowed to do with their information. Today the most commonly used terms of use and licensing agreements give companies the right to do what they wish with consumers’ information as a condition of using the service. If consumers enter “accept” once prompted—and they must do that before being able to utilize a service—they likely have very limited rights. Manufacturers and service providers should work with consumer representatives, including associations and the FTC, to standardize these agreements for clarity and appropriateness.

While standardizing the presentation of information about consumer rights relating to the purchase of a particular device or service would be a positive development, it is not enough to protect and inform consumers concerning cybersecurity and privacy. The Commission recommends that consumer organizations work with industry and the FTC to develop a consumer “cybersecurity bill of rights and responsibilities” that would:

- simplify consumer education on their rights;
- provide insights on what technology vendors and providers are legally allowed to do with consumer information;
- clarify privacy protections;
- articulate responsibilities of all citizens that participate in the digital economy; and,
- identify the security attributes of products and services.

This bill of rights and responsibilities should be disseminated widely in order to increase consumers' awareness of their roles in the responsible use of digital devices and networks, including the consequences that an individual's actions have for others in the larger digital economy.

Recommendation 3.2: The federal government should establish, strengthen, and broaden investments in research programs to improve the cybersecurity and usability of consumer products and digital technologies through greater understanding of human behaviors and their interactions with the Internet of Things (IoT) and other connected technologies.

Human interactions with computing technologies and devices have a direct impact on cybersecurity. Often, the privacy and security protections built into the designs of products are difficult to use or require multiple steps that encourage users to develop workarounds to circumvent those privacy and cybersecurity features that would protect them. Ease of use must be a key consideration in product development. Additional and ongoing research in this area of human interaction will help designers and manufacturers understand how secure, easy-to-use products can be created.

***Action Item 3.2.1:** The next Administration and Congress should prioritize research on human behavior and cybersecurity, on the basis of the 2016 Federal Cybersecurity Research and Development Strategic Plan. (SHORT TERM)*

The Office of Science and Technology Policy (OSTP) coordinated the development of a federal cybersecurity R&D plan that points out the need to identify and teach human behaviors that enhance security.²⁴ The plan also makes clear that we need to identify effective methods to encourage more cyber-secure behavior in the design and operation of IT systems. Further attention is given to this issue in the context of research in *Imperative 2, Action Item 2.2.2*.

24 National Science and Technology Council, Networking and Information Technology Research and Development Program, "Federal Cybersecurity Research and Development Strategic Plan: Ensuring Prosperity and National Security," February 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf.

Imperative 4: Build Cybersecurity Workforce Capabilities

The Challenge and Way Forward

Meeting the critical national and economic security need to expand and strengthen an agile cybersecurity workforce will require a national effort that engages all levels of the public sector as well as the private sector. According to “The 2015 (ISC)² Global Information Security Workforce Study,” 1.5 million more cybersecurity professionals will be needed globally by 2020.²⁵ Cybersecurity offers a premium in pay over other fields in information technology, yet a sizable gap between open positions and qualified applicants has persisted for almost a decade. Both the quantity and the quality of those applying for positions remain significant problems, as does the challenge of ensuring that training is up-to-date and effective. One recent study found that most entry-level staff lack the necessary technical skills and, as a result, 86 percent of employers must provide on-the-job training.²⁶

In addition, an increasing number of occupations will demand some level of cybersecurity knowledge. Within the United States, there are millions of companies and businesses, tens of thousands of local governments and public school systems, and hundreds of millions of personal computer users. This growing number includes members of the workforce at all levels, with mid- and senior-level managers among those who will need to regularly improve their cybersecurity skills. It is just as important that the general workforce and executives receive training as it is that cybersecurity professionals be recruited and kept current. Every one of these organizations and people will need a baseline knowledge of cybersecurity to perform their jobs effectively.

To address the shortage, we must expand our current efforts to draw more workers into the cybersecurity field. The workforce shortage in cybersecurity is directly related to a larger problem:

too few high school and college students in the United States are developing the skills necessary for careers in science, technology, engineering, and mathematics (STEM). Even while more is being done to encourage and sustain interest in STEM, the economic and national security of the United States cannot wait a decade or longer for initiatives in primary and secondary education to bear fruit. Closing the gap in the near term will require a national surge that increases the workforce and provides a structure for on-the-job training to ensure that the current workforce has the right skill set. This surge would benefit both the private and public sectors by increasing the number of employee candidates who are qualified to address urgent cybersecurity needs. Moreover, movement between sectors would benefit all concerned, especially over time as cybersecurity specialists gain experience in different environments and domains.

To increase the number of qualified entry-level cybersecurity practitioners, the federal government must work with the private sector to attract more students to the field of cybersecurity. These collaborative efforts also should aim to create pathways into the field for underrepresented populations (e.g., women, minorities, and veterans) and older workers seeking career changes or hoping to leave professions with fewer opportunities. The current focus on retraining veterans for careers in cybersecurity should be continued and expanded.

The Commission recognizes the possibility that advances in automation, artificial intelligence, and machine learning may slow (and possibly reverse) the demand for more workers in the field; however, the Commission also notes that cybersecurity work roles and responsibilities are increasingly being integrated into a growing array of jobs at all levels with nearly all organizations. Unlike the skills needed for jobs in other sectors, such as manufacturing or retail, a strong technical grounding in cybersecurity will create opportunities for employment in a number of different types of jobs in the current and future digital economy. In addition, the effects of automation, machine learning, and artificial intelligence on cybersecurity workforce demand will likely not be realized by most enterprises for several years or longer; the nation needs to surge its cybersecurity workforce today.

25 “The 2015 (ISC)² Global Information Security Workforce Study,” Frost & Sullivan White Paper, 2015, p.3, [www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-\(ISC\)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf](http://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf).

26 “State of Cybersecurity: Implications for 2016,” p.12, An ISACA and RSA Conference Survey, 2016, http://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf.

This report, like many assessments of our nation's cybersecurity needs, tends to focus on the number of cybersecurity professionals and the education and training programs required to meet our current and future needs. The Commissioners also note, however, that some of the most important advances in organizations' cybersecurity derive from the work of creative individuals who develop new concepts and approaches to address cybersecurity challenges. No formula or specific recommendation can lead to their breakthroughs, and such efforts cannot be quantified—but it is important to ensure that we continue to create environments that encourage and reward them. Encouraging innovation, which is one of the foundational principles of this report, has made the United States the global leader in technological innovation, especially in driving the Information Revolution.

Workforce recommendations related to federal, state, local, tribal, and territorial governments, including enlisting the capabilities of the National Guard, are provided below and in *Imperative 5, Action Item 5.5.3*. Many of these recommendations build on the Federal Cybersecurity Workforce Strategy that OMB and the Office of Personnel Management (OPM) issued in July 2016 and will further the goals outlined in that strategy.

Recommendation 4.1: The nation should proactively address workforce gaps through capacity building, while simultaneously investing in innovations—such as automation, machine learning, and artificial intelligence—that will redistribute the future required workforce.

The cybersecurity workforce is expected to continue to grow over the next several years, but not at a rate commensurate with the growing threats. Consequently, we need to continue to expand existing initiatives and develop new ones that will grow our nation's workforce.

Building on current successful efforts is an important first step. The National Science Foundation (NSF) supports capacity building in institutions of higher education through the CyberCorps: Scholarship for Service program.²⁷ This federal program's success has resulted in the establishment of complementary state models, such as the Virginia Cybersecurity Public Service

Scholarship.²⁸ The Cybersecurity National Action Plan (CNAP)²⁹ also contains new cybersecurity education and workforce initiatives, including enhancements to student loan forgiveness programs for cybersecurity experts joining the federal workforce. The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework,³⁰ published recently by NIST, identifies several broad categories of cybersecurity work, with more than 30 specialty areas and more than 50 work roles. The federal government is using the NICE Framework to assess its current cybersecurity workforce and identify gaps as required by the Federal Cybersecurity Workforce Assessment Act of 2015.³¹

These programs, and others that have been successful, should be scaled up and grown, with funding increased to a level commensurate with the scale of the national workforce shortage.

Action Item 4.1.1: *The next President should initiate a national cybersecurity workforce program to train 100,000 new cybersecurity practitioners by 2020. (SHORT TERM)*

A national cybersecurity workforce program would help our nation develop cybersecurity talent pipelines. Such a program—with a specific focus on local and regional partnerships of employers, educational institutions, and community organizations—will help develop the skilled workforce necessary to meet the cybersecurity needs of local and regional industry. One successful example is the TechHire initiative,³² launched by the White House in 2015, which expands local technology sectors by providing technology talent pipelines in communities across the country.

The federal government and private-sector partners should also jointly sponsor a nationwide network of cybersecurity boot camps. Aimed at providing knowledge and skills in a condensed

28 "Governor McAuliffe Announces \$1 Million in Cybersecurity Scholarships," Virginia.gov, August 19, 2016, <https://governor.virginia.gov/newsroom/newsarticle?articleId=16192>.

29 The White House, Office of the Press Secretary, "FACT SHEET: Cybersecurity National Action Plan," February 9, 2016, <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>.

30 Available at National Institute for Cybersecurity Education, "NICE Cybersecurity Workforce Framework," <http://csrc.nist.gov/nice/framework/>.

31 Chief Human Capital Officers Council, "Requirements of the Federal Cybersecurity Workforce Assessment Act," August 1, 2016, <https://www.chcoc.gov/content/requirements-federal-cybersecurity-workforce-assessment-act>.

32 "TechHire Initiative," <https://www.whitehouse.gov/issues/technology/techhire>.

27 U.S. Office of Personnel Management, "CyberCorps®: Scholarship for Service" (expires 3/31/2017), <https://www.sfs.opm.gov/>.

time frame, these training initiatives will increase the supply of practitioners and allow the redeployment of individuals who are currently underemployed or unemployed. Boot camps also are an excellent way to identify underrepresented populations of cybersecurity workers, such as women and minorities, and to develop targeted recruitment and training efforts in cohorts that maximize the opportunity for completing the program and transitioning into the workforce.

Action Item 4.1.2: *The next President should initiate a national cybersecurity apprenticeship program to train 50,000 new cybersecurity practitioners by 2020.* (MEDIUM TERM)

The program should have pathways for students in traditional four-year university programs and two-year community college programs with a specific focus on developing the skills necessary to begin a career in cybersecurity. The program should also have a specific focus on developing, outside of traditional academic settings, the skills necessary to begin a career in cybersecurity. The initiative should promote the development of entry-level and mid-level skills—including in students graduating with engineering, computing, or IT degrees with excellent technical skills but little actual cybersecurity training—followed by hands-on apprenticeships both in government and in the private sector.

Action Item 4.1.3: *To better prepare students as individuals and future employees, federal programs supporting education at all levels should incorporate cybersecurity awareness for students as they are introduced to and provided with Internet-based devices.* (SHORT TERM)

Cybersecurity awareness messages should be developed and focused on children as early as preschool and throughout elementary school. This early cybersecurity education must include programs to train and better prepare teachers in order to succeed at scale. Successful programs, such as the NSF- and National Security Agency (NSA)-run GenCyber,³³ which provides summer cybersecurity camp experiences for students and teachers at the K-12 level, should be leveraged to help all students understand safe online behavior and to increase diversity and interest in cybersecurity careers. This effort would also stimulate exploration of cybersecurity careers in middle school

and enable preparedness for cybersecurity careers in high school. In addition, the process of exposing young people to technology and the associated safety, security, ethical, and legal issues will introduce them to a broad range of academic and career pathways that can sustain lifelong employment.

Action Item 4.1.4: *The federal government should develop a mandatory training program to introduce managers and executives to cybersecurity risk management topics—even if their role is not focused on a cybersecurity mission area—so that they can create a culture of cybersecurity in their organizations.* (SHORT TERM)

To successfully address and integrate cyber risks within a risk management framework, agency leaders need to have sufficient knowledge of cyber risks, threat mitigation strategies, cyber performance metrics, and related factors—regardless of their agency mission—because cybersecurity is a core part of every agency’s mission. In this sense, such knowledge is no different than the basic finance, procurement, human resources, and other business skills expected of every senior leader within an agency. However, little priority has been given to seeking government executives or agency leaders with these skills, or providing individuals the opportunity to develop them. In the near term, the knowledge, skills, and experience needed for cyber risk management should be integrated into the executive training and development programs for all federal agencies—in effect, a “cyber-MBA” should be designed for government executives. The Senior Executive Service (SES) should be prioritized to receive this training; cyber risk elements should be systematically incorporated into SES training, selection, performance evaluation, and professional development. Such programs are well defined within federal agencies, and these executives are often the primary interface between the program specialists and the political leadership of a department or agency. The training then should be expanded to other management levels.

Action Item 4.1.5: *The federal government, SLTT governments, and private-sector organizations should create an exchange program aimed at increasing the cybersecurity experience and capabilities of mid-level and senior-level employees.* (SHORT TERM)

33 See GenCyber, “Inspiring the Next Generation of Cyber Stars,” <https://www.gen-cyber.com/>.

Both the public sector and the private sector are experiencing an acute cybersecurity workforce shortage. One of the most important attributes of a cybersecurity worker is the experience she or he obtains while on the job—whether working in government or in industry.

Rotational assignments within the government or private sector are starting to be recognized as a best practice for retention. These assignments lay the groundwork for a surge capacity, making it possible to deploy individuals quickly and flexibly as situations warrant. This exchange program should embrace innovative approaches to workforce management, including support for virtual employment exchanges, and seek to streamline administrative processing and address potential barriers to participation that could hinder private-sector rotations into the federal government (e.g., security clearance processing, existing/potential contract relationships, regulatory actions).

Action Item 4.1.6: *The Office of Personnel Management (OPM) should establish a Presidential Cybersecurity Fellows program for federal civilian agencies with the goal of bringing on 200 cybersecurity specialists by 2020. (SHORT TERM)*

Aspiring and seasoned cybersecurity managers and leaders are in high demand in government and industry alike. To attract more managers and senior leaders to federal government service, OPM should establish Presidential Cybersecurity Fellows through a program similar to the Presidential Management Fellows program, but focused on cybersecurity. Through a competitive application process, this program would bring individuals into government and place them in cybersecurity positions with responsibilities relating both to technology and policy areas. The program would be open to students who recently completed graduate programs and to faculty or seasoned professionals. For students or mid-career professionals, this program would provide career development opportunities and expose a new generation of aspiring leaders to the possibilities and rewards of a career in federal government service, as a cybersecurity technology or policy specialist.

Action Item 4.1.7: *NIST, the National Science Foundation (NSF), the National Security Agency (NSA), and the Department of Education should work with private-sector organizations, universities, and professional societies to develop standardized interdisciplinary cybersecurity curricula that integrate with and expand existing efforts and programs. (MEDIUM TERM)*

As the cybersecurity profession continues to evolve and mature, so too do efforts to create curricula, degree programs, and certificates of study in cybersecurity. There is a wide range of academic options, as various cybersecurity and privacy degrees, certificates, and concentrations have emerged. Many efforts are now underway to develop curricular guidance for cybersecurity, such as work undertaken by the Association for Computing Machinery and the Institute of Electrical and Electronics Engineers Joint Task Force on Cybersecurity Education³⁴ and a new curriculum effort led by NSA under CNAP.³⁵ The NSA/DHS Centers of Academic Excellence in Cybersecurity³⁶ are incentivizing institutions to map their curriculum and degree programs to knowledge units aligned to NIST's National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.³⁷

Despite these nascent endeavors, including similar initiatives at the high school level, no common body of knowledge or core curriculum has yet been agreed on or widely adopted. We need a concerted national effort to inventory existing curricula and initiatives, identify gaps, and develop and disseminate a standardized set of guidelines and resources to guide teachers and administrators. This effort should also pursue collaborations with organizations that accredit college and university programs in scientific, engineering, and computing disciplines, such as the Accreditation Board for Engineering and Technology (ABET).³⁸ Cybersecurity should be a basic requirement for the accreditation of any programs in engineering and computing disciplines.

Action Item 4.1.8: *In order to attract more students to pursue cybersecurity degree programs and enter the cybersecurity workforce in both the public and private sectors, incentives*

34 "ACM Joint Task Force on Cybersecurity Education," <http://www.csec2017.org/>.

35 The White House, Office of the Press Secretary, "FACT SHEET: Cybersecurity National Action Plan," February 9, 2016, <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>.

36 NSA/CSS, "Resources for Educators: Centers of Academic Excellence in Cybersecurity," May 3, 2016, <https://www.nsa.gov/resources/educators/centers-academic-excellence/>.

37 Bill Newhouse, Stephanie Keith, Benjamin Scribner, and Greg Witte, "NICE Cybersecurity Workforce Framework (NCWF): National Initiative for Cybersecurity Education (NICE)," Draft NIST Special Publication 800-181, November 2016, http://csrc.nist.gov/publications/drafts/800-181/sp800_181_draft.pdf.

38 ABET website, <http://www.abet.org/>.

should be offered to reduce student debt or subsidize the cost of education through a public–private partnership. (MEDIUM TERM)

The increase in the cost of college and in student debt is an enormous public policy challenge. The private sector should structure a program that provides financial support (i.e., scholarships, loan forgiveness, tuition reimbursement) for students who earn vocational, polytechnic, or master’s degrees in related cybersecurity fields. Specifically, in exchange for a period of service within the federal government, followed by a period of employment at a sponsoring company, that company will cover education expenses (e.g., student aid). The program would help the federal government to address a significant talent deficit and would provide the private sector with a pool of experienced cybersecurity professionals who possess federal government relationships and experience.

This page intentionally left blank.

Imperative 5: Better Equip Government to Function Effectively and Securely in the Digital Age

The Challenge and Way Forward

The federal government faces two challenges in cybersecurity. First, it is a major user of information technology in providing essential government services of all types, and in all agencies. The government is therefore highly dependent on a reliable, secure, and connected cyber infrastructure. Second, many federal agencies have specific roles in protecting and defending the country, including its citizens, businesses, and infrastructure, from cyber attack, and in responding to catastrophic cyber incidents. In both of these areas, the government has faced challenges, as demonstrated by the Office of Personnel Management (OPM) breach in 2015.³⁹ But in the face of rapidly changing information technology capability and a growing dependence on this technology, it is not enough for the next Administration to try to play catch-up with threats and vulnerabilities. The next President must ensure that the federal government is a leader in cybersecurity, both to secure its own operational systems and to carry out its mission to protect and defend our nation's private networks when a major incident occurs.

Recent Administration efforts, coupled with congressional action, provide a foundation for necessary improvements in how the federal government functions in the digital age and how it manages its own house—but more must be done, purposefully and quickly. Significant cyber incidents and high-visibility breaches have underscored the seriousness and urgency of the situation for the federal government—and its impact on the rest of the nation.

Cybersecurity must be made a national security priority equal to counterterrorism and protection of the homeland. If the federal government is to lead, the next President must empower and expect accountability from the officials charged with overseeing implementation of the national strategy. To drive home this point, the President should be explicit about the priority of cybersecurity in discussions with his cabinet; in his initial full meeting with

these leaders, the President should make clear that they will be held accountable for their agencies' cybersecurity. He also should elevate cybersecurity responsibilities within the Executive Office of the President.

The government must be better organized and better resourced for this purpose. Protecting federal information and systems must be an unquestionable Administration priority. Departments and agencies must receive clear direction and necessary resources, and leaders must have the mechanisms to set and enforce policy. Aside from clarifying its responsibilities for operating government agencies and services, the federal government must also explain with greater clarity its mission focus, by delineating the roles and responsibilities of government in protecting the private sector.

Recommendation 5.1: The federal government should take advantage of its ability to share components of the information technology (IT) infrastructure by consolidating basic network operations.

To be effective and secure in the digital age, every organization requires a modern, defensible network architecture. Today, nearly every civilian agency procures and manages its own IT infrastructure, from the connection to the Internet to endpoint devices and software. While this independence enables agencies to optimize how IT supports their mission, it fails to take advantage of certain aspects of the IT infrastructure that work better at scale when managed as a shared resource. Two areas, in particular, would benefit: providing secure and reliable Internet connectivity to federal agencies, and procuring standard devices and services. If basic network access is consolidated into a single agency high-performance network, then connectivity can be provided effectively and efficiently within a framework of robust network security infrastructure and support. The government gains from connecting agencies to the Internet through a centralized, monitored, and trustworthy network environment, and agencies benefit by not having to invest in dedicated network operations and security functions beyond those they need for local area networks.

³⁹ OPM, Cybersecurity Resource Center, "What Happened," <https://www.opm.gov/cybersecurity/cybersecurity-incidents>.

Action Item 5.1.1: *The Administration should establish a program to consolidate all civilian agencies' network connections (as well as those of appropriate government contractors) into a single consolidated network. This program and the consolidated network should be administered by the newly established cybersecurity and infrastructure protection agency described in Action Item 5.5.2. (MEDIUM TERM)*

The new agency should develop and implement a program to provide secure, reliable network services to all civilian government agencies, thereby providing a consolidated network for all .gov entities. Working closely with the Assistant to the President for Cybersecurity (see Action Item 5.4.1) and the Federal Chief Information Officer (CIO), the agency should establish and monitor security performance requirements that agencies on this consolidated network must meet in order to connect. To protect the integrity of this network, the agency should have the authority to modify or remove connected devices, services, or agencies that fail to meet those requirements.

In exchange for meeting these requirements, federal agencies on the network should be guaranteed a high-quality connection and baseline level of performance. To this end, the new agency administering the network must be responsible for establishing and meeting clear performance standards. Oversight of the consolidated network's performance levels should be provided by the Federal CIO, Federal Chief Information Security Officer (CISO), and the CIO Council.

Recommendation 5.2: The President and Congress should promote technology adoption and accelerate the pace at which technology is refreshed within the federal sector.

Strengthening cybersecurity in federal operations requires major changes in the way government agencies approach the issue. It requires thorough implementation of improved standards, guidelines, and best practices, as well as a more agile and capable workforce in numbers matched to the size of the task at hand. (See multiple action items under Imperative 4, including recommendations to develop executive leadership training programs on cyber risk management as well as specific steps needed to strengthen identity management.) It demands a culture attuned to and rewarded for innovation.

The government has a serious legacy IT problem. Too many agencies are patching systems and hoping that the latest fix will keep their older systems working and secure, even though

older technologies have much poorer security functionality. The government loses both ways: it introduces substantial vulnerabilities and it fails to benefit from new features and functionality. In short, the government's "refresh rate" of reinvestment in dated IT systems is much slower than the rate of innovation and improvement in IT. The government needs to modernize and to ensure that this modernization can be sustained at a faster pace. This modernization will be costly, but will bring very large gains in security and performance.

Modern, world-class cybersecurity operations that actively manage the kinds of threats faced by federal agencies also require good planning and predictable funding. Budget planning and acquisition cycles are not aligned with budget authorizations or annual appropriations. Federal IT security budgets should be structured around a multiyear strategy to enable more rational planning and operations. To this end, the executive branch and Congress should identify cybersecurity priorities that can be resourced even when federal funding is subject to continuing resolutions. These changes should allow agencies to fully integrate cybersecurity into overall program funding rather than addressing them as "add on" costs.

The Administration and Congress must look critically at the disparity between the millions of dollars spent by the federal government on threat mitigation and the billions of dollars spent less cost-effectively on IT security and vulnerability mitigation.

The true cost of operating IT is not being considered by the federal government. Funding requests should fully account for operating costs rather than just initial procurement costs.

The next President should formally announce his intention to increase investment in modernizing federal IT. The United States stands on the edge of the next generation of information technology innovation, including advances in big data capacities, machine learning, artificial intelligence, and new computing fabrics such as quantum and bio computing. But federal agencies will have a hard time taking advantage of those improvements due to constrained resources and inadequate long-term planning. Adding to the challenge, it is also crucial that the technologies adopted by federal agencies today not lock these agencies out of the capabilities of tomorrow. Newer systems should be modular and agile in order to prepare them for inevitable changes in the future.

In addition, the government should take advantage of the opportunity to share aspects of the IT infrastructure by consolidating procurement responsibility for standard endpoint devices and services.

Action Item 5.2.1: *The Administration should expand on the recently proposed Information Technology Modernization Fund (ITMF) to enable agencies to fund technology investments by spreading costs over a predetermined period of time. The investments made under this fund should be integrated into a rolling 10-year strategic investment plan as part of a budget planning process similar to the Department of Defense (DoD) approach. (SHORT TERM)*

An important step in this direction was taken in 2016 with the proposal of a \$3.1 billion ITMF as part of the Administration's CNAP.⁴⁰ The ITMF would facilitate the retirement, replacement, and modernization of legacy IT that is difficult to secure and expensive to maintain. Agencies would be required to repay funds received from the ITMF over the time needed to refresh new technology, not the period defined by the technology's "useful life." This approach results in a more aggressive reinvestment period of 5 to 7 years, rather than the current 10+-year timeframe. The fund is self-sustaining and minimizes large and irregular increases to agency budgets to fund technology reinvestment.

Recognizing the urgency of this issue and the opportunity for a major shift in how the government addresses its IT and cybersecurity needs, the Commission recommends expanding that fund so that more agencies can take fuller advantage of this investment mechanism.

It is essential that the federal government devise and adhere to a rolling 10-year strategic IT investment plan. Some of the most deeply rooted issues the federal government grapples with in relation to cybersecurity are tied to the process constraints of the federal budget, which too often lead agencies to repair legacy systems as the default option. These expenditures are reactionary, as opposed to the kinds of forward-thinking planning that is needed to deliver a fast, reliable, and secure federal IT infrastructure. OMB should work with departments and agencies

to integrate this longer-term planning into the current Capital Planning and Investment Control process and update budgetary requirements as needed.

Action Item 5.2.2: *The General Services Administration (GSA) should lead efforts on integrating technology more effectively into government operations, working with Congress to reform federal procurement requirements and expanding the use of sharing standard service platforms. (MEDIUM TERM)*

Beyond the issue of investment planning, GSA should lead the Administration's work with Congress to reform federal procurement requirements for IT-related purchases to maximize effectiveness of procurement and adapt the federal acquisition process to reflect the dynamic and rapidly evolving nature of IT. Specifically:

- approval by agency CISOs should be required in advance of all IT investments related to the security of agency data and systems (a responsibility not of GSA but of each agency);
- GSA and other agencies should use integrated teams of technologists and acquisition experts; and,
- GSA should reform the procurement protest regime in order to decrease the delays in obtaining necessary products and services, thereby better managing cybersecurity risk.

Additional technology acquisition reforms should be explored. Possible models are DoD's Defense Innovation Unit - Experimental (DIUx) and the R&D and rapid acquisition programs of the Defense Advanced Research Projects Agency (DARPA), the Intelligence Advanced Research Projects Activity (IARPA), and the Air Force's Rapid Capabilities Office (RCO).

Furthermore, GSA should expand the development and use of standard service platforms (e.g., endpoint devices, shared data clouds, software as a service) to provide agencies with high-performance infrastructure and tools for their mission, while minimizing direct agency responsibility for managing and operating the infrastructure. Greater sharing of services, such as web hosting, standard software, and common cloud services, would enable government to take advantage of its scale to negotiate and obtain higher-performance and lower-cost IT equipment and services. By sharing, agencies can focus on aspects of the IT infrastructure that most directly address

⁴⁰ White House, "FACT SHEET: Cybersecurity National Action Plan," February 9, 2016, <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>.

their mission. They retain the authority and responsibility for optimizing IT services to meet their mission needs, and benefit from the embedded security features that are part of their network and shared procurement.

Recommendation 5.3: Move federal agencies from a cybersecurity requirements management approach to one based on enterprise risk management (ERM).

For too long, federal agency cybersecurity requirements have been viewed as a checklist wholly separate from an agency's core functions and capabilities. There has been a tendency to emphasize strict compliance with prescriptive requirements rather than enterprise risk management. Efforts have been made, especially over the past several years, to stress the value of risk management using standards, guidelines, and best practices developed for federal agencies. However, the federal government has failed to adopt this risk management approach. Instead, it has focused on implementing specific, prescriptive requirements. The Commission recommends that the federal government adopt a risk management approach guided by OMB's enterprise risk management program.⁴¹

As part of this effort, federal agencies should be required to use the Cybersecurity Framework as a common standard to evaluate their cybersecurity posture and integrate cybersecurity with the agency's mission. Such an approach would help eliminate the misperception that cybersecurity is auxiliary to, rather than a core part of, every agency's mission. It would properly put discussions of cybersecurity risk on the same level as other enterprise-wide risks. It would also reinforce the move away from a culture concerned only with meeting minimum standards.

Action Item 5.3.1: *The Office of Management and Budget (OMB) should require federal agencies to use the Cybersecurity Framework for any cybersecurity-related reporting, oversight, and policy review or creation.* (SHORT TERM)

It is vital that the federal government adopt and implement proven best practices from the private sector, other governments, and standards bodies. NIST has published guidance to map the Cybersecurity Framework (developed in conjunction with the

private sector) to the Risk Management Framework (RMF) that OMB expects agencies to use.⁴² The two frameworks align, and the Commission believes strongly that there is no reason that agencies should not be using the Cybersecurity Framework for multiple purposes. To that end, NIST should build on its past work and produce one or more "profiles" to assist agencies in using the Cybersecurity Framework.

NOTE: Other Commission recommendations urging more extensive use of the Cybersecurity Framework appear below and in *Imperative 1, Recommendation 1.4*.

Action Item 5.3.2: *In the first 100 days of the Administration, OMB should work with NIST and DHS to clarify agency and OMB responsibilities under the Federal Information Security Modernization Act (FISMA) to align with the Cybersecurity Framework.* (SHORT TERM)

The Federal Information Security Modernization Act, along with its associated implementation policies, standards, and guidelines, imposes requirements and expectations on federal agencies as they manage cybersecurity risk. At times, these requirements compete and conflict with one another, or quickly become outdated as a result of technological advances and a rapidly changing threat landscape. OMB, working with NIST and DHS, should identify and address areas of alignment between the Cybersecurity Framework and existing federal requirements. This effort should address areas of conflict or overlap in existing requirements for federal agencies, and gap areas where additional policies, standards, guidelines, and programs may be needed to improve the ability of federal agencies to manage cybersecurity risk.

Specifically, the Federal CISO should conduct a complete and comprehensive review of all current OMB cybersecurity requirements. At a minimum, these requirements should include OMB memos, binding operational directives, reporting instructions, and audit directions. Requirements that are no longer effective, are in conflict with current presidential priorities, or are outdated should be withdrawn. All new policies should be structured using the Cybersecurity Framework to ensure

41 Executive Office of the President, Office of Management and Budget, "OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control," July 15, 2016, <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-17.pdf>.

42 National Institute of Standards and Technology, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," NIST Special Publication 800-37, Revision 1, February 2010 (includes updates as of 06-05-2014), <http://dx.doi.org/10.6028/NIST.SP.800-37r1>.

consistency in reporting and assessments. In addition, OMB should give serious consideration to canceling programs that have proven not to be effective.

Action Item 5.3.3: *OMB should integrate cybersecurity metrics with agency performance metrics, review these metrics biannually, and integrate metrics and associated performance with the annual budget process. (SHORT TERM)*

It is often said that the devil is in the details; when it comes to assessing cybersecurity preparedness, the devil is in the metrics. One of the greatest challenges to determining cybersecurity strength has been a lack of standards of measurement. Metrics, in combination with a risk management approach, will provide a foundation for effectively evaluating, understanding, and improving the cybersecurity posture of agencies.

To address this need, the Commission recommends that the Cybersecurity Framework Metrics Working Group (CFMWG)—a body drawing on both the public and private sectors, within the proposed National Private–Public Partnership (NCP³)—develop metrics to assess an entity’s cybersecurity posture. The metrics will be valuable for all sectors, and should be fully embraced by OMB and federal agencies in their efforts to better quantify and evaluate the effectiveness of their actions. These metrics should be integrated with other measures used to assess performance as part of the annual budget process. (More information about the CFMWG is provided in *Imperative 1, Action Item 1.4.1.*)

Recommendation 5.4: The federal government should better match cybersecurity responsibilities with the structure of and positions in the Executive Office of the President.

The current leadership and organizational construct for cybersecurity within the federal government is not commensurate with the challenge of securing the digital economy and supporting the national and economic security of the United States.

Effective implementation of cybersecurity priorities will require strong leadership, beginning at the top. Some important steps toward improving national cybersecurity have been taken, such as appointing the first-ever Federal Chief Information Security Officer and establishing a privacy branch, led by a career official in the OMB Office of Information and Regulatory Affairs. Additional improvements are needed.

The next President should identify cybersecurity as a top national

security priority, and should empower his officials charged with overseeing that priority accordingly. The mission must be resourced sufficiently and the government must be staffed and organized to carry it out.

One key part of that mission is protecting federal information and systems. Agencies must receive clear direction from the President and be granted corresponding authorities. All agency heads must understand that cybersecurity is one of their essential responsibilities. Where appropriate, the President should use the power of executive orders to deliver directives to the executive branch, including to ensure that responsibility, authority, and accountability for cybersecurity are properly aligned at the government-wide level and within each agency. Each and every federal employee and contractor must understand and work in a way that is consistent with this basic tenet.

Action Item 5.4.1: *The President should appoint and empower an Assistant to the President for Cybersecurity, reporting through the National Security Advisor, to lead national cybersecurity policy and coordinate implementation of cyber protection programs. (SHORT TERM)*

Cybersecurity must become and remain an essential priority in how the federal government does business. This focus and resolve will require strong leadership. The Commission recommends that the President elevate the current position of Cybersecurity Coordinator to an Assistant to the President, on par with the Assistant to the President for Homeland Security and Counterterrorism. He or she should have responsibility for bringing together the federal government’s efforts to protect its own systems and data and to secure the larger digital economy, and should inform and coordinate with the Director of OMB on efforts by the Federal CIO and CISO to secure federal agencies.

Action Item 5.4.2: *The Administration should clarify OMB’s role—and specifically, that of the Federal Chief Information Officer (CIO), the Federal Chief Information Security Officer (CISO), and the Senior Advisor for Privacy—in managing cybersecurity-related operations in all agencies. (SHORT TERM)*

OMB plays a central role in ensuring that federal agencies operate their information technology securely and effectively, and that an effective risk management approach is used to carry out their mission. This role is carried out through the Federal CIO, and is supported by the CISO, along with privacy policy leadership currently provided by the Senior Advisor for Privacy. High priority

must be given to laying out clear outcome-focused requirements to drive agency priorities. This effort requires these officials to work with Congress and agency leaders to ensure that an appropriate budget is allocated to meet those priorities, and to develop and maintain a rigorous risk management framework for agencies to address cybersecurity risks that can threaten their mission.

The Commission recommends that the Federal CIO conduct a rolling assessment of the government's cybersecurity performance on a quarterly basis to ensure a sustained level of performance on fundamental cybersecurity actions. He or she must make certain that agencies systematically identify and prioritize their highest value and most at-risk IT assets. Adherence to minimum cybersecurity standards must be better monitored, reported, and enforced than it is today. The President should make clear that the Federal CIO will lead this effort in the federal government.

The Federal CIO, working in consultation with the Federal CISO, the Senior Advisor for Privacy, the Assistant to the President for Cybersecurity, and the head of the new agency charged with cybersecurity and infrastructure protection functions (see *Action Item 5.5.2* below), should identify similar baseline security measures that can be implemented immediately.

The recently established position of Federal CISO is a meaningful addition to OMB's capability in this area. The Federal CISO should be granted appropriate and clear authority by the Federal CIO to support the above responsibilities. The Federal CISO should also serve as a primary connection between the efforts of OMB and of the Assistant to the President for Cybersecurity. If the Federal CISO is appropriately included in these national security activities, all federal agencies will benefit from the latest risk and threat information.

Similarly, OMB's capability to coordinate governance of personal data has benefited from the recently established position of Senior Advisor for Privacy to the Director of OMB, and the role of this policy official in leading the Federal Privacy Council. This policy official has led OMB's privacy policy work; in addition, a lead career official for privacy has been created in the OMB Office of Information and Regulatory Affairs. Because many issues concerning personal data have both cybersecurity and privacy implications, it is important to retain a policy official focused on privacy in order to ensure proper consideration of the privacy aspects of cybersecurity policy across the federal government.

Recommendation 5.5: Government at all levels must clarify its cybersecurity mission responsibilities across departments and agencies to protect and defend against, respond to and recover from cyber incidents.

Governments need to have a clear understanding of their roles and responsibilities to more effectively and consistently prepare and plan for, respond to, and recover from cyber incidents. This clear understanding will ensure improved government coordination and more efficient use of resources; it will promote the strengthening of existing capabilities and help identify the new ones we need to build.

Action Item 5.5.1: *The President should issue a National Cybersecurity Strategy within the first 180 days of his Administration. (SHORT TERM)*

This comprehensive cybersecurity strategy should set forth the vision and priorities for achieving security and resilience in cyberspace. The strategy should include the creation of a defensible national cyber architecture and should provide a roadmap for implementation and policy development that can guide the national effort to secure the digital economy over the next decade.

Action Item 5.5.2: *Congress should consolidate cybersecurity and infrastructure protection functions under the oversight of a single federal agency, and ensure this agency has the appropriate capabilities and responsibilities to execute its mission. (SHORT TERM)*

Consistent with the national cybersecurity strategy called for in Action Item 5.5.1, Congress should create a new component agency, or repurpose an existing agency, to serve as a fully operational cybersecurity and critical infrastructure protection agency on par with other component agencies. This agency should be solely dedicated to these two core missions, and it should be given the necessary authorities, responsibilities, and resources to carry out these missions effectively.

Working closely with the Assistant to the President for Cybersecurity (See Action Item 5.4.1) and the Federal Chief Information Officer (CIO), this agency should establish and administer the consolidated federal network described in Action Item 5.1.1, including establishing criteria that federal agencies must meet in order to connect to this network. The agency must also guarantee federal agencies using the consolidated

network, a high-quality and reliable level of service. To this end, it should establish and adhere to clear performance metrics for the network. To ensure the agency is accountable for providing this level of service, Congress should provide a mechanism by which the Federal Chief Information Officer (CIO), Federal Chief Information Security Officer (CISO), and CIO Council may oversee the agency's performance.

In addition to administering the consolidated federal network, this agency would monitor and assess information technology trends across the digital economy, with an emphasis on critical infrastructure. This tasking would help address the limited capability within the federal government to monitor and assess these trends in the United States and gauge how they might affect the cybersecurity of critical infrastructure, consumers, and the federal government.

Action Item 5.5.3: *The governors in each state should consider seeking necessary legislative authority and resources to train and equip the National Guard to serve as part of the nation's cybersecurity defense. (SHORT–MEDIUM TERM)*

In some states, the National Guard today provides much-needed expertise to assist states in tackling their most pressing cybersecurity challenges. The Guard represents a talent pool that can be regularly trained, equipped, and called on to protect and defend against attacks on information assets or computer systems and networks. The Guard could also be deployed after a cybersecurity incident to help recover or restore systems and services to normal operations. Building on recent and growing investments in developing sophisticated cyber defense capabilities in the National Guard, state legislatures should give serious consideration to providing governors with the necessary authorities and resources to train and equip the National Guard to serve their states and safeguard the public from malicious cyber activity.

The Commission recognizes that governors approach cybersecurity by engaging a diverse set of senior officials and enterprises, including some combination of the National Guard and their chief information officer, homeland security director, emergency management director, and chief security officer. The Commission recommends that states should continue to engage a team of leaders in addressing cybersecurity challenges and strategies.

This page intentionally left blank.

Imperative 6: Ensure an Open, Fair, Competitive, and Secure Global Digital Economy

The Challenge and Way Ahead

The United States operates in a global economy with partners, suppliers, customers, and competitors around the world. Business is now conducted at Internet speeds in digital markets and does not stop at boundaries or borders. The digital economy also depends on an open, interoperable, secure, and reliable Internet that links every corner of the globe. This globally connected economy relies on a patchwork of technology requirements, regulations, policies, and laws that can be at odds with the free and instantaneous flow of information. Coordinated and effective international harmonization and cooperation are needed in order to realize the full economic promise of the nation and the world, and to allow for the efficient flow of information and ideas. The unprecedented economic and social opportunities created for individuals and organizations by this global network must be balanced against the needs of each country to protect itself from fraud, abuse, crime, and security threats. Each nation also has the right to defend itself appropriately in cyberspace.

Today, the international digital economy lacks the coherent systems necessary to effectively address cross-border malicious cyber activity. The varied individual country technology requirements, assessment regimes, and cybersecurity policies fragment markets and force companies to devote resources to multiple compliance regimes rather than to innovation. The lack of global norms and standards forces industry to select markets where they can meet national requirements, avoiding or abandoning others. The lack of structure adds to disparities that can degrade national cybersecurity capabilities. The void in technical, policy, and legal conventions hampers information sharing and interoperability. Moreover, it creates an opening for criminals to launch attacks and conduct other malicious cyber activity.

The obvious but hard-to-achieve desired state is an international system of systems that values responsible state behavior, discourages activity that is destabilizing to the global networks, and promotes the growth of the digital economy, domestically and abroad. Mechanisms need to be developed to build the capacity of partner states to investigate and prosecute cybercrime within

their borders and to increase the cybersecurity of their critical systems. Continued collaboration and cooperation, building on a significant effort over the past two years, is required to develop common standards and assessment activities and to harmonize regional and global cybersecurity and privacy policies, laws, and norms.

Recommendation 6.1: The Administration should encourage and actively coordinate with the international community in creating and harmonizing cybersecurity policies and practices and common international agreements on cybersecurity law and global norms of behavior.

The transnational nature of the Internet makes international cooperation essential to an effective and secure global digital economy. Issues that need to be addressed internationally include the development of cybersecurity and technical standards, international conformance requirements, and coordinated incident response; increased multilateral legal cooperation; continued progress toward international consensus on applying international law to cyberspace; and formalization of communications channels.

Large global companies—and smaller companies active in trade—face an increasing number of cybersecurity-focused regulatory requirements from jurisdictions around the world. Confronted with competing, sometimes redundant, and even conflicting regulatory obligations, these companies can find themselves allocating disproportionate resources to reconciling requirements, such as cybersecurity certifications and cybersecurity examination questionnaires, when their efforts would be more productively spent on actual cybersecurity measures. Advancing a harmonized approach for developing cybersecurity and technology requirements would aid significantly in promoting the adoption of meaningful cybersecurity measures. This approach would also reduce and avoid the regulatory and compliance burden imposed by numerous competing regulatory requirements and ad hoc, conflicting compliance mandates. The business community would also benefit from the increased predictability, which is essential for further investment of resources in cybersecurity efforts.

Action Item 6.1.1: *Within the first 180 days of the next Administration, the President should appoint an Ambassador for Cybersecurity to lead U.S. engagement with the international community on cybersecurity strategies, standards, and practices.* (SHORT TERM)

To further communicate to the international community that cybersecurity is a top U.S. national security priority, the Commission believes that the President should appoint a senior official as ambassador to coordinate and lead U.S. engagement on cybersecurity. This position would be on par with the newly created Assistant to the President for Cybersecurity and would elevate this issue within the Department of State. The newly created ambassador position should be empowered to speak and act on the Secretary of State's behalf and have a direct line to the Secretary. This individual should have responsibility for bringing together international counterparts to harmonize cybersecurity standards and practices, and to develop and promote peacetime norms of nation-state behavior and a common understanding of the application of international law in cyberspace. The ambassador would also have the authority to negotiate and oversee the implementation of confidence-building measures on a bilateral and multilateral basis.

Action Item 6.1.2: *The federal government should increase its engagement in the international standards arena to garner consensus from other nations and promote the use of sound, harmonized cybersecurity standards.* (MEDIUM TERM)

Decisions made in the international standards arena have important consequences for the cybersecurity of devices and systems, and the federal government should better coordinate and more actively participate in these efforts. This engagement, which must be coordinated with industry in accordance with federal statute and policies, should focus on cybersecurity and privacy standards that increase security and privacy while fostering interoperability. These standards must win consensus from multiple nations and markets.

In accordance with an OMB policy directive (OMB A-119),⁴³ the Director of NIST chairs the Interagency Committee on Standards

Policy, which includes the lead privacy official at OMB, the Department of State, the Department of Commerce's International Trade Administration, the Department of Homeland Security, and the U.S. Trade Representative. This forum should be used by the federal government to guide and improve coordination and expand U.S. international standards participation.

The Commission recommends a dedicated initiative to better align cybersecurity standards activities. This effort should include increasing the U.S. government role in developing international cybersecurity standards, and it should begin with vigorous efforts to promote use of the Cybersecurity Framework for international partners, including international regulators. (See *Imperative 1, Recommendation 1.4.*)

Action Item 6.1.3: *The Department of State should continue its work with like-minded nations to promote peacetime cybersecurity norms of behavior.* (SHORT TERM)

The Department of State should build on current efforts with allies and other countries that share similar cybersecurity concerns to develop a strategy for expanding the adoption of cybersecurity norms of behavior in cyberspace during peacetime.

The State Department should identify venues of opportunity, including in bilateral and regional engagements, the United Nations' Group of Governmental Experts, the G7, the G20, the Organization of Security Co-operation in Europe (OSCE) and Organisation for Economic Co-operation and Development (OECD), and other multilateral forums. The Administration should make this strategy a cornerstone of its international engagements to ensure stability in cyberspace, open access to markets, the free exchange of ideas, and the stability of the digital economy.

Action Item 6.1.4: *Congress should provide sufficient resources to the Department of Justice (DOJ) to fully staff and modernize the Mutual Legal Assistance Treaty (MLAT) process, including hiring engineers and investing in technology that enables efficiency. It should also amend U.S. law to facilitate transborder access to electronic evidence for limited legitimate investigative purposes, and should provide resources for the development of a broader framework and standards to enable this transborder access.* (MEDIUM TERM)

43 Office of Management and Budget, Executive Office of the President, revision of OMB Circular No. A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities," January 27, 2016, https://www.whitehouse.gov/sites/default/files/omb/infomag/revise/circular_a-119_as_of_1_22.pdf.

U.S. companies provide electronic communications services globally, including to many subjects of foreign law enforcement investigations. When the communications data for those persons are stored or accessible only in the United States, a conflict can arise between the requirements of U.S. laws and of the foreign country's laws. The MLAT process was designed to facilitate the lawful fulfillment of foreign law enforcement requests for information and evidence, but it was designed for another era, with far fewer requests, before electronic evidence was routinely stored in other countries, such as in cloud services; it lacks the speed, agility, and resources needed to stop today's criminals. Dissatisfaction with the MLAT process has fueled calls by many countries for data localization, which would harm the U.S. technology industry and impede development of new global Internet services.

In addition to reforming the MLAT process and increasing DOJ funding to support it, Congress should pass legislation proposed by the Administration⁴⁴ that provides a speedier alternative for qualifying governments to obtain extraterritorial communications data related to preventing, detecting, investigating, or prosecuting serious crimes. The United States and United Kingdom have negotiated a bilateral agreement that eliminates conflicts of laws so that each nation, under certain conditions, may have its requests for copies of data honored by companies in the other nation. However, in order to implement the agreement, legislative changes are necessary, including establishing a broader framework and the standards to implement that framework that will be needed to bring numerous countries into similar agreements. In order to ensure that such agreements are reciprocal, and to meet the needs of U.S. law enforcement investigations, Congress should also ensure that in appropriate

circumstances, U.S. law authorizes law enforcement to obtain electronic data located abroad.

Action Item 6.1.5: *NIST and the Department of State should proactively seek international partners to extend the Cybersecurity Framework's approach to risk management to a broader international market. (SHORT TERM)*

NIST, in coordination with other sector-specific agencies (e.g., the Departments of Energy, Transportation, and Treasury), should proactively expand U.S. participation and leadership in the development of international cybersecurity standards for industry and other nations. The Department of State should identify partners to help extend this approach globally. The United States has developed important cybersecurity risk management approaches that could benefit organizations here and abroad. Developing and selecting international standards is an increasingly important element of many nations' economic strategy, and the United States has a corresponding opportunity to enhance the capabilities of those participating nations. In particular, NIST should promote the use of the Cybersecurity Framework by actively working with industry to seek its acceptance in international standards bodies.

Action Item 6.1.6: *The Department of State, DHS, and other agencies should continue to assist countries with cybersecurity capacity building in light of growing needs and recent developments. (SHORT TERM)*

The United States can more effectively respond to foreign cyber threats when our international partners have their own strong cybersecurity capabilities, in planning, preparation, and response. U.S. cybersecurity and privacy capacity building is essential in creating international partners with common interoperable technologies, policies, and supportive laws to ensure the security of the global digital economy. This assistance includes helping other nations to use internationally accepted standards and conformance programs in building their cybersecurity capabilities, and to adhere to and enforce international laws. Capacity building will help improve cybersecurity threat and vulnerability information sharing, as well as supply chain security, attack identification and attribution, and cooperation in critical infrastructure protection. The federal government should review its existing capacity-building efforts, identify any gaps that exist, and develop solutions to fill those gaps. It should then coordinate with other nations to provide capacity building where

44 The Department of Justice has proposed legislation that would permit direct access to U.S. providers pursuant to agreements entered into between the executive branch and governments that meet specified criteria. These criteria are designed to ensure that only countries that afford robust substantive and procedural protections for privacy and civil liberties will be permitted to request data directly from U.S.-based companies. In return, the United States would be assured reciprocal access to data abroad for its law enforcement investigations. A recent U.S. court decision held that the federal government could not require companies storing data in another nation to provide copies of that data to the government based solely on a U.S. warrant. *Microsoft Corp. v. United States*, No. 14-2985 (2d Cir. 2016), <http://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412>. If that decision stands and its reasoning is adopted by other federal courts, the United States may not have the authority to avail itself of this benefit, and the proposed agreements would not be reciprocal.

most needed. These efforts will require increased resources from Congress.

Moreover, the expanded capacity-building strategy should be supported by an implementation plan that coordinates funding and programs across the many agencies that invest in the capacity of other nations, including but not limited to the Departments of State, Homeland Security, Defense, and Justice. The strategy and implementation plan should be informed by and, where applicable, organized according to the Cybersecurity Framework, so that all parties can focus on a standardized set of cybersecurity outcomes.

IV. Next Steps

When President Obama charged this Commission with developing recommendations for enhancing national cybersecurity, he conveyed an extreme sense of urgency—a sentiment with which this Commission agrees. Improving our state of cybersecurity is a top national priority, for both the private and public sectors.

It is critical that the next President and his Administration and Congress begin immediately to tackle each one of the issues raised in this report. The Commission considers this report a direct memo to the next President. The recommendations reflect what the Commissioners believe are the highest-priority actions to take. Some recommendations call for actions within the first 100 days of the new Administration.

It is important that the next Administration prepare, in short order, a cohesive, thorough plan for implementing these recommendations, building on the specific action items identified in this report. The private sector should be consulted and involved in preparing this plan. This process must be launched and completed in a compressed time frame. Importantly, the next Administration must increase funding for cybersecurity across the federal government.

Metrics that focus on outcomes should be part of the action plan. Results matter, and simply taking action is not nearly enough. Worse yet, focusing solely on actions can create the illusion of meaningful progress and impacts when little has actually changed.

Recognizing that the next President and Administration will bear the burden of leadership in following up on most of this report's recommendations, the Commission also believes firmly that there is much that industry and the private sector, as well as government agencies at all levels, can and must do immediately. Seeing the steep upward trend in malicious cyber activity and mindful of the serious nature of cyber risks, organizations and individuals are taking steps to improve their own cybersecurity. At the same time, recent initiatives appropriately call for ambitious measures to put the federal government's cybersecurity house in order. Momentum to do so should not be slowed as the next Administration assumes power.

Simply put, no agency, no company, no individual should delay efforts to improve their digital security and resilience while the Commission's recommendations are being considered.

This page intentionally left blank.

Appendix 1: Imperatives, Recommendations, and Action Items

NOTE: Some recommendations apply to more than the single imperative under which they first appear.

| Imperative 1 | Protect, Defend, and Secure Today's Information Infrastructure and Digital Networks |
|--------------------|--|
| Recommendation 1.1 | The private sector and the Administration should collaborate on a roadmap for improving the security of digital networks, in particular by achieving robustness against denial-of-service, spoofing, and other attacks on users and the nation's network infrastructure. |
| Action Item 1.1.1 | The President should direct senior federal executives to launch a private–public initiative, including provisions to undertake, monitor, track, and report on measurable progress in enabling agile, coordinated responses and mitigation of attacks on the users and the nation's network infrastructure. (SHORT TERM) |
| Recommendation 1.2 | As our cyber and physical worlds increasingly converge, the federal government should work closely with the private sector to define and implement a new model for how to defend and secure this infrastructure. |
| Action Item 1.2.1 | The President should create, through executive order, the National Cybersecurity Private–Public Program (NCP ³) as a forum for addressing cybersecurity issues through a high-level, joint public—private collaboration. (SHORT TERM) |
| Action Item 1.2.2 | The private sector and Administration should launch a joint cybersecurity operation program for the public and private sectors to collaborate on cybersecurity activities in order to identify, protect from, detect, respond to, and recover from cyber incidents affecting critical infrastructure (CI). (MEDIUM TERM) |
| Action Item 1.2.3 | The federal government should provide companies the option to engage proactively and candidly in formal collaboration with the government to advance cyber risk management practices and to establish a well-coordinated joint defense plan based on the principles of the Cybersecurity Framework. (SHORT TERM) |
| Action Item 1.2.4 | Federal agencies should expand the current implementation of the information-sharing strategy to include exchange of information on organizational interdependencies within the cyber supply chain. (SHORT TERM) |
| Action Item 1.2.5 | With the increase in wireless network communications across all organizations, and the nation's growing reliance on the Global Positioning System (GPS) to provide positioning, navigation, and timing (PNT), cybersecurity strategies must specifically address the full range of risks across the electromagnetic spectrum. An immediate goal should be enhancing the nation's ability to detect and resolve purposeful wireless disruptions and to improve the resilience and reliability of wireless communications and PNT data. (SHORT TERM) |

| | |
|--------------------|---|
| Recommendation 1.3 | The next Administration should launch a national public–private initiative to achieve major security and privacy improvements by increasing the use of strong authentication to improve identity management. |
| Action Item 1.3.1 | The next Administration should require that all Internet-based federal government services provided directly to citizens require the use of appropriately strong authentication. (SHORT TERM) |
| Action Item 1.3.2 | The next Administration should direct that all federal agencies require the use of strong authentication by their employees, contractors, and others using federal systems. (SHORT TERM) |
| Action Item 1.3.3 | The government should serve as a source to validate identity attributes to address online identity challenges. (MEDIUM TERM) |
| Action Item 1.3.4 | The next Administration should convene a body of experts from the private and public sectors to develop identity management requirements for devices and processes in support of specifying the sources of data. (SHORT TERM) |
| Recommendation 1.4 | The next Administration should build on the success of the Cybersecurity Framework to reduce risk, both within and outside of critical infrastructure, by actively working to sustain and increase use of the Framework. |
| Action Item 1.4.1 | NIST, in coordination with the NCP ³ , should establish a Cybersecurity Framework Metrics Working Group (CFMWG) to develop industry-led, consensus-based metrics that may be used by (1) industry to voluntarily assess relative corporate risk, (2) the Department of Treasury and insurers to understand insurance coverage needs and standardize premiums, and (3) DHS to implement a nationwide voluntary incident reporting program for identifying cybersecurity gaps. This reporting program should include a cyber incident data and analysis repository (CIDAR). (SHORT TERM) |
| Action Item 1.4.2 | All federal agencies should be required to use the Cybersecurity Framework. (SHORT TERM) |
| Action Item 1.4.3 | Regulatory agencies should harmonize existing and future regulations with the Cybersecurity Framework to focus on risk management—reducing industry’s cost of complying with prescriptive or conflicting regulations that may not aid cybersecurity and may unintentionally discourage rather than incentivize innovation. (SHORT TERM) |
| Action Item 1.4.4 | The private sector should develop conformity assessment programs that are effective and efficient, and that support the international trade and business activities of U.S. companies. (SHORT TERM) |
| Action Item 1.4.5 | The government should extend additional incentives to companies that have implemented cyber risk management principles and demonstrate collaborative engagement. (SHORT TERM) |

| | |
|---------------------|--|
| Recommendation 1.5 | The next Administration should develop concrete efforts to support and strengthen the cybersecurity of small and medium-sized businesses (SMBs). |
| Action Item 1.5.1 | The National Institute of Standards and Technology (NIST) should expand its support of SMBs in using the Cybersecurity Framework and should assess its cost-effectiveness specifically for SMBs. (SHORT TERM) |
| Action Item 1.5.2 | DHS and NIST, through the National Cybersecurity Center of Excellence (NCCoE), in collaboration with the private sector, should develop blueprints for how to integrate and use existing cybersecurity technologies, with a focus on meeting the needs of SMBs. (SHORT TERM) |
| Action Item 1.5.3 | Sector-specific agencies (SSAs) and industry associations and organizations should collaborate to develop a program to review past public cyber attacks to identify lessons learned from the event, including a focus on application to SMBs. (SHORT TERM) |
| Imperative 2 | Innovate and Accelerate Investment for the Security and Growth of Digital Networks and the Digital Economy |
| Recommendation 2.1 | The federal government and private-sector partners must join forces rapidly and purposefully to improve the security of the Internet of Things (IoT). |
| Action Item 2.1.1 | To facilitate the development of secure IoT devices and systems, within 60 days the President should issue an executive order directing NIST to work with industry and voluntary standards organizations to identify existing standards, best practices, and gaps for deployments ranging from critical systems to consumer/commercial uses—and to jointly and rapidly agree on a comprehensive set of risk-based security standards, developing new standards where necessary. (SHORT TERM) |
| Action Item 2.1.2 | Regulatory agencies should assess whether effective cybersecurity practices and technologies that are identified by the standards process in Action Item 2.1.1 are being effectively and promptly implemented to improve cybersecurity and should initiate any appropriate rule making to address the gaps. (MEDIUM TERM) |
| Action Item 2.1.3 | The Department of Justice should lead an interagency study with the Departments of Commerce and Homeland Security and work with the Federal Trade Commission, the Consumer Product Safety Commission, and interested private-sector parties to assess the current state of the law with regard to liability for harm caused by faulty IoT devices and provide recommendations within 180 days. (SHORT TERM) |
| Action Item 2.1.4 | The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) should develop and communicate guidelines for IoT cybersecurity and privacy best practices for rapid deployment and use. (SHORT TERM) |

| | |
|---------------------|--|
| Recommendation 2.2 | The federal government should make the development of usable, affordable, inherently secure, defensible, and resilient/recoverable systems its top priority for cybersecurity research and development (R&D) as a part of the overall R&D agenda. |
| Action Item 2.2.1 | The Director of the Office of Science and Technology Policy (OSTP) should lead the development of an integrated government–private-sector cybersecurity roadmap for developing usable, affordable, inherently secure, resilient/recoverable, privacy-protecting, functional, and defensible systems. This effort should be backed by a significant R&D funding increase in the President’s Budget Request for agencies supporting this roadmap. (SHORT TERM) |
| Action Item 2.2.2 | The U.S. government should support cybersecurity-focused research into traditionally underfunded areas, including human factors and usability, policy, law, metrics, and the social impacts of privacy and security technologies, as well as issues specific to small and medium-sized businesses where research can provide practical solutions. (SHORT TERM) |
| Imperative 3 | Prepare Consumers to Thrive in a Digital Age |
| Recommendation 3.1 | Business leaders in the information technology and communications sectors need to work with consumer organizations and the Federal Trade Commission (FTC) to provide consumers with better information so that they can make informed decisions when purchasing and using connected products and services. |
| Action Item 3.1.1 | To improve consumers’ purchasing decisions, an independent organization should develop the equivalent of a cybersecurity “nutritional label” for technology products and services—ideally linked to a rating system of understandable, impartial, third-party assessment that consumers will intuitively trust and understand. (SHORT AND MEDIUM TERM) |
| Action Item 3.1.2 | Within the first 100 days of the new Administration, the White House should convene a summit of business, education, consumer, and government leaders at all levels to plan for the launch of a new national cybersecurity awareness and engagement campaign. (SHORT TERM) |
| Action Item 3.1.3 | The FTC should convene consumer organizations and industry stakeholders in an initiative to develop a standard template for documents that inform consumers of their cybersecurity roles and responsibilities as citizens in the digital economy—along with a “Consumer’s Bill of Rights and Responsibilities for the Digital Age.” (MEDIUM TERM) |
| Recommendation 3.2 | The federal government should establish, strengthen, and broaden investments in research programs to improve the cybersecurity and usability of consumer products and digital technologies through greater understanding of human behaviors and their interactions with the Internet of Things (IoT) and other connected technologies. |

| | |
|---------------------|--|
| Action Item 3.2.1 | The next Administration and Congress should prioritize research on human behavior and cybersecurity, on the basis of the 2016 Federal Cybersecurity Research and Development Strategic Plan. (SHORT TERM) |
| Imperative 4 | Build Cybersecurity Workforce Capabilities |
| Recommendation 4.1 | The nation should proactively address workforce gaps through capacity building, while simultaneously investing in innovations—such as automation, machine learning, and artificial intelligence—that will redistribute the future required workforce. |
| Action Item 4.1.1 | The next President should initiate a national cybersecurity workforce program to train 100,000 new cybersecurity practitioners by 2020. (SHORT TERM) |
| Action Item 4.1.2 | The next President should initiate a national cybersecurity apprenticeship program to train 50,000 new cybersecurity practitioners by 2020. (MEDIUM TERM) |
| Action Item 4.1.3 | To better prepare students as individuals and future employees, federal programs supporting education at all levels should incorporate cybersecurity awareness for students as they are introduced to and provided with Internet-based devices. (SHORT TERM) |
| Action Item 4.1.4 | The federal government should develop a mandatory training program to introduce managers and executives to cybersecurity risk management topics—even if their role is not focused on a cybersecurity mission area—so that they can create a culture of cybersecurity in their organizations. (SHORT TERM) |
| Action Item 4.1.5 | The federal government, SLTT governments, and private-sector organizations should create an exchange program aimed at increasing the cybersecurity experience and capabilities of mid-level and senior-level employees. (SHORT TERM) |
| Action Item 4.1.6 | The Office of Personnel Management (OPM) should establish a Presidential Cybersecurity Fellows program for federal civilian agencies with the goal of bringing on 200 cybersecurity specialists by 2020. (SHORT TERM) |
| Action Item 4.1.7 | NIST, the National Science Foundation (NSF), the National Security Agency (NSA), and the Department of Education should work with private-sector organizations, universities, and professional societies to develop standardized interdisciplinary cybersecurity curricula that integrate with and expand existing efforts and programs. (MEDIUM TERM) |
| Action Item 4.1.8 | In order to attract more students to pursue cybersecurity degree programs and enter the cybersecurity workforce in both the public and private sectors, incentives should be offered to reduce student debt or subsidize the cost of education through a public-private partnership. (MEDIUM TERM) |

| Imperative 5 | Better Equip Government to Function Effectively and Securely in the Digital Age |
|---------------------|--|
| Recommendation 5.1 | The federal government should take advantage of its ability to share components of the information technology (IT) infrastructure by consolidating basic network operations. |
| Action Item 5.1.1 | The Administration should establish a program to consolidate all civilian agencies' network connections (as well as those of appropriate government contractors) into a single consolidated network. This program and the consolidated network should be administered by the newly established cybersecurity and infrastructure protection agency described in Action Item 5.5.2. (MEDIUM TERM) |
| Recommendation 5.2 | The President and Congress should promote technology adoption and accelerate the pace at which technology is refreshed within the federal sector. |
| Action Item 5.2.1 | The Administration should expand on the recently proposed Information Technology Modernization Fund (ITMF) to enable agencies to fund technology investments by spreading costs over a predetermined period of time. The investments made under this fund should be integrated into a rolling 10-year strategic investment plan as part of a budget planning process similar to the Department of Defense (DoD) approach. (SHORT TERM) |
| Action Item 5.2.2 | The General Services Administration (GSA) should lead efforts on integrating technology more effectively into government operations, working with Congress to reform federal procurement requirements and expanding the use of sharing standard service platforms. (MEDIUM TERM) |
| Recommendation 5.3 | Move federal agencies from a cybersecurity requirements management approach to one based on enterprise risk management (ERM). |
| Action Item 5.3.1 | The Office of Management and Budget (OMB) should require federal agencies to use the Cybersecurity Framework for any cybersecurity-related reporting, oversight, and policy review or creation. (SHORT TERM) |
| Action Item 5.3.2 | In the first 100 days of the Administration, OMB should work with NIST and DHS to clarify agency and OMB responsibilities under the Federal Information Security Modernization Act (FISMA) to align with the Cybersecurity Framework. (SHORT TERM) |
| Action Item 5.3.3 | OMB should integrate cybersecurity metrics with agency performance metrics, review these metrics biannually, and integrate metrics and associated performance with the annual budget process. (SHORT TERM) |
| Recommendation 5.4 | The federal government should better match cybersecurity responsibilities with the structure of and positions in the Executive Office of the President. |
| Action Item 5.4.1 | The President should appoint and empower an Assistant to the President for Cybersecurity, reporting through the National Security Advisor, to lead national cybersecurity policy and coordinate implementation of cyber protection programs. (SHORT TERM) |

| | |
|---------------------|---|
| Action Item 5.4.2 | The Administration should clarify OMB's role—and specifically, that of the Federal Chief Information Officer (CIO), the Federal Chief Information Security Officer (CISO), and the Senior Advisor for Privacy—in managing cybersecurity-related operations in all agencies. (SHORT TERM) |
| Recommendation 5.5 | Government at all levels must clarify its cybersecurity mission responsibilities across departments and agencies to protect and defend against, respond to and recover from cyber incidents. |
| Action Item 5.5.1 | The President should issue a National Cybersecurity Strategy within the first 180 days of his Administration. (SHORT TERM) |
| Action Item 5.5.2 | Congress should consolidate cybersecurity and infrastructure protection functions under the oversight of a single federal agency, and ensure this agency has the appropriate capabilities and responsibilities to execute its mission. (SHORT TERM) |
| Action Item 5.5.3 | The governors in each state should consider seeking necessary legislative authority and resources to train and equip the National Guard to serve as part of the nation's cybersecurity defense. (SHORT-MEDIUM TERM) |
| Imperative 6 | Ensure an Open, Fair, Competitive, and Secure Global Digital Economy |
| Recommendation 6.1 | The Administration should encourage and actively coordinate with the international community in creating and harmonizing cybersecurity policies and practices and common international agreements on cybersecurity law and global norms of behavior. |
| Action Item 6.1.1 | Within the first 180 days of the next Administration, the President should appoint an Ambassador for Cybersecurity to lead U.S. engagement with the international community on cybersecurity strategies, standards, and practices. (SHORT TERM) |
| Action Item 6.1.2 | The federal government should increase its engagement in the international standards arena to garner consensus from other nations and promote the use of sound, harmonized cybersecurity standards. (MEDIUM TERM) |
| Action Item 6.1.3 | The Department of State should continue its work with like-minded nations to promote peacetime cybersecurity norms of behavior. (SHORT TERM) |
| Action Item 6.1.4 | Congress should provide sufficient resources to the Department of Justice (DOJ) to fully staff and modernize the Mutual Legal Assistance Treaty (MLAT) process, including hiring engineers and investing in technology that enables efficiency. It should also amend U.S. law to facilitate transborder access to electronic evidence for limited legitimate investigative purposes, and should provide resources for the development of a broader framework and standards to enable this transborder access. (MEDIUM TERM) |
| Action Item 6.1.5 | NIST and the Department of State should proactively seek international partners to extend the Cybersecurity Framework's approach to risk management to a broader international market. (SHORT TERM) |
| Action Item 6.1.6 | The Department of State, DHS, and other agencies should continue to assist countries with cybersecurity capacity building in light of growing needs and recent developments. (SHORT TERM) |

This page intentionally left blank.

Appendix 2: List of Public Meetings and Agendas

This appendix lists all public meetings held by the Commission followed by the meeting agendas. For more details on each meeting, including its Federal Register notice and minutes, see <https://www.nist.gov/cybercommission/commission-meetings>.

| Date | Location |
|--------------------|---|
| April 14, 2016 | U.S. Department of Commerce, Washington, DC |
| May 16, 2016 | New York University School of Law, New York, NY |
| June 21, 2016 | University of California, Berkeley, Berkeley, CA |
| July 14, 2016 | University of Houston, Houston, TX |
| August 23, 2016 | University of Minnesota, Minneapolis, MN |
| September 19, 2016 | American University Washington College of Law, Washington, DC |
| November 21, 2016 | Public Teleconference |

| Thursday, April 14, 2016, U.S. Department of Commerce, Washington, DC |
|--|
| Welcome <ul style="list-style-type: none"> Penny Pritzker, U.S. Secretary of Commerce |
| Introductory Remarks and Commissioner Introduction <ul style="list-style-type: none"> Thomas E. Donilon, Commission Chair, O’Melveny & Myers, Vice Chair; Former U.S. National Security Advisor to President Obama Samuel J. Palmisano, Commission Vice Chair, Retired Chairman and CEO, IBM Corporation |
| Ethics Briefing and FACA Briefing <ul style="list-style-type: none"> Gaye Williams, Department of Commerce, Office of the General Counsel, Deputy Chief, Ethics Law and Programs Division Alice McKenna, Department of Commerce, Office of the General Counsel, Senior Counsel |
| White House Briefing <ul style="list-style-type: none"> Lisa Monaco, White House, Assistant to the President for Homeland Security and Counterterrorism |
| Commission Scope of Work Discussion |
| Review of Commission Timeline |
| Public Comment |
| Meeting Adjourned |

Monday, May 16, 2016, New York University School of Law, New York, NY

Welcome

- Zachary K. Goldman, Executive Director, Center on Law & Security; Adjunct Professor of Law, New York University School of Law; Co-Founder, NYU Center for Cybersecurity
- Trevor Morrison, Dean, Eric M. and Laurie B. Roth Professor of Law, New York University School of Law

Panel 1: Finance

- Phil Venables, Managing Director and CISO, Goldman Sachs
- Greg Rattray, Managing Director, Head of Global Cyber Partnerships, JP Morgan Chase
- Marc Gordon, Executive Vice President and CIO, American Express

Break

Panel 2: Insurance

- Lee Garvin, Director of Risk Management and Workers Compensation, JetBlue Airways
- Peter Beshar, Executive Vice President and General Counsel, Marsh & McLennan Companies, Inc.
- Randal Milch, Former General Counsel, Verizon; Distinguished Fellow, NYU School of Law
- Catherine Mulligan, Senior Vice President, Head of Professional Liability, Zurich North America

Lunch

Panel 3: Research and Development

- Irving Wladawsky-Berger, Visiting Lecturer, Sloan School of Management, MIT; Strategic Advisor, MasterCard; Executive in Residence, New York University; Adjunct Professor, Imperial College, London
- Alex Pentland, Professor, MIT
- Jerry Cuomo, IBM Fellow, VP Blockchain Technologies
- Greg Baxter, Global Head of Digital, Citi

Commission Discussion

Public Comment

Meeting Adjourned

Tuesday, June 21, 2016, University of California, Berkeley, Berkeley, CA

Welcome

- Betsy Cooper, Executive Director, Center for Long-Term Cybersecurity, UC-Berkeley
- Nils Gilman, Associate Chancellor, UC-Berkeley

Meeting Opening and Remarks

- Thomas E. Donilon, Commission Chair, O'Melveny & Myers, Vice Chair; Former U.S. National Security Advisor to President Obama
- Samuel J. Palmisano, Commission Vice Chair, Retired Chairman and CEO, IBM Corporation

Panel 1: Addressing Security Challenges to the Digital Economy

- Geoff Belknap, CISO, Slack
- Patrick Heim, Chief Trust Officer, Dropbox
- Hemma Prafullchandra, EVP and Chief Technology Officer, Products, HyTrust
- Alex Stamos, CISO, Facebook

Break

Panel 2: Collaborating to Secure the Digital Economy

- Thomas Andriola, Vice President & CIO, University of California System
- Dr. Cynthia Dwork, Distinguished Scientist, Microsoft Research
- Eric Grosse, Vice President, Security Engineering, Google
- Eli Sugarman, Cyber Initiative Program Officer, The William and Flora Hewlett Foundation

Lunch

Panel 3: Innovating to Secure the Future of the Digital Economy

- Gilman Louie, Partner, Alsop Louie Partners, former CEO, In-Q-Tel
- Mark McLaughlin, Chair, National Security Telecommunications Advisory Committee (NSTAC); Chairman, President and CEO, Palo Alto Networks
- Ted Schlein, Managing Partner, Kleiner Perkins Caufield & Byers (KPCB)

Public Comment

Center for Long-Term Cybersecurity (CLTC) Briefing

- Steve Weber, Faculty, School of Information, UC-Berkeley

Commission Discussion

Meeting Adjourned

Thursday, July 14, 2016, University of Houston, Houston, TX

Welcome and Overview

- Dr. Paula Myrick Short, Senior Vice Chancellor for Academic Affairs, University of Houston System; Senior Vice President for Academic Affairs and Provost, University of Houston
- Marty Edwards, Director, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), a division of the National Cybersecurity and Communications Integration Center (NCCIC) in the Department of Homeland Security

Panel 1: Current and Future Effect of Critical Infrastructure on the Digital Economy

- Robert "Bob" Kolasky, Deputy Assistant Secretary, Office of Infrastructure Protection, U.S. Department of Homeland Security
- Steve Mustard, Cybersecurity Committee Chair, Automation Federation
- Dr. Subhash Paluru, Senior VP & Sierra Nevada Regional Manager, Western Area Power Administration
- Mark Webster, Assistant Special Agent in Charge, FBI-Houston Division

Break

Panel 2: Critical Infrastructure Cybersecurity Challenges Affecting the Digital Economy

- Scott Aaronson, Executive Director, Security and Business Continuity, Edison Electric Institute (EEI); Member of the Secretariat, Electricity Subsector Coordinating Council (ESCC)
- Chris Boyer, Assistant Vice President, Global Public Policy, AT&T Services Inc.
- Dr. Wm. Arthur "Art" Conklin, Director, University of Houston, Center for Information Security Research and Education
- Scott Robichaux, Cyber Security Manager, ExxonMobil GSC Information Management

Lunch

Panel 3: Cybersecurity Challenges and Opportunities in State and Local Governments

- Edward Block, CISO, State of Texas, Texas Department of Information Resources
- Major General Reynold N. Hoover, Director of Intelligence for the Chief of the National Guard Bureau; Director of Command, Control, Communications, and Computers and Chief Information Officer, National Guard Bureau
- David Laplander, CISSP, CISO, Houston IT Services, City of Houston

Public Comment

Commission Discussion

Meeting Adjourned

Tuesday, August 23, 2016, University of Minnesota, Minneapolis, MN

Welcome and Overview

- Dr. Massoud Amin, Director, Chair, Technological Leadership Institute; Distinguished University Professor, University of Minnesota

Panel 1: Consumers and the Digital Economy

- Susan Grant, Director, Consumer Protection and Privacy, Consumer Federation of America
- Mike Johnson, Director of Graduate Studies in Security Technologies, Technological Leadership Institute, University of Minnesota
- Kevin Moriarty, Senior Attorney, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission (FTC)
- Sarah Zatko, Chief Scientist, Cyber Independent Testing Laboratory (CITL)

Break

Panel 2: Innovation (Internet of Things, Healthcare, and Other Areas)

- Robert Booker, Senior VP, Chief ISO, UnitedHealth Group, Optum, Inc.
- Brian McCarson, CTO, Intel IoT Strategy; Sr. Principal Engineer, Chief Architect, Intel IoT Platform
- Gary Toretti, Chief ISO, Sabre Corporation

Lunch

Panel 3: Assured Products and Trustworthy Technologies

- Edna Conway, CSO, Global Value Chain, Cisco Systems, Inc.
- Joshua Corman, Director, Cyber Statecraft Initiative; Former CTO, Sonatype; Co-Founder, I am The Cavalry and Rugged Software
- Ken Modeste, Global Cybersecurity Technical and Strategy Lead, Underwriters Laboratories Inc. (UL)
- Dr. Ron Ross, Computer Scientist, National Institute of Standards and Technology (NIST)

Public Comment

Commission Discussion

Meeting Adjourned

Monday, September 19, 2016, American University School of Law, Washington, DC

Welcome and Overview

- Camille Nelson, Dean, American University Washington College of Law
- John Delaney, Dean, Kogod School of Business (KSB) at American University
- Rebekah Lewis, Deputy Director, Kogod Cybersecurity Governance Center (KCGC)

Meeting Opening

- Penny Pritzker, Secretary of Commerce, U.S. Department of Commerce

International Discussion

- Chris Painter, Coordinator for Cyber Issues, U.S. Department of State

Panel 1: How Did We Get to Here? The Policies That Shape Today's Federal IT Landscape

- Dan Chenok, Executive Director, Center for the Business of Government, IBM
- Karen Evans, National Director, U.S. Cyber Challenge; Former CIO, U.S. Government
- Eric Fischer, Senior Specialist in Science and Technology, Congressional Research Service (CRS)
- Gregory C. Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office (GAO)

Readout from the August 3, 2016, Subcommittee Meeting

Lunch

Panel 2: Growing and Securing the Digital Economy

- Alan Davidson, Director of Digital Economy, U.S. Department of Commerce; Senior Advisor, Secretary of Commerce
- Rick Geritz, CEO, LifeJourney
- Mike Walker, Program Manager, Information Innovation Office, Defense Advanced Research Projects Agency (DARPA)
- Neal L. Ziring, Technical Director, Capabilities Directorate, National Security Agency (NSA)

Panel 3: Embracing Innovation in the Government and Preparing for the Future

- Dr. Evan Cooke, Senior Policy Advisor, Office of Science and Technology Policy, The White House
- Tom Donahue, Research Director, Cyber Threat Intelligence Integration Center
- Eric Mill, Senior Advisor on Technology, Technology Transformation Service, U.S. General Services Administration (GSA)
- Mark Ryland, Chief Solutions Architect, World Wide Public Sector Team, Amazon Web Services (AWS)

Public Comment

Commission Discussion

Meeting Adjourned

Monday, November 21, 2016, Public Teleconference

Meeting Opening

- Kiersten Todt, Executive Director

Opening Remarks

- Thomas E. Donilon, Commission Chair, O'Melveny & Myers, Vice Chair; Former U.S. National Security Advisor to President Obama
- Samuel J. Palmisano, Commission Vice Chair, Retired Chairman and CEO, IBM Corporation

Approval of Public Meeting Minutes

- Kiersten Todt, Executive Director

Briefing and readout of three working group meetings (9/20, 10/19, 11/8)

- Maggie Wilderotter, Commissioner
- Pat Gallagher, Commissioner
- Steve Chabinsky, Commissioner

Public Comment

Conclusion

- Thomas E. Donilon, Commission Chair, O'Melveny & Myers, Vice Chair; Former U.S. National Security Advisor to President Obama

This page intentionally left blank.

Appendix 3: Request for Information (RFI) Submissions

On August 10, 2016, a request for information (RFI)⁴⁵ was posted to solicit information from the public for the Commission on the following topics:

- Critical infrastructure cybersecurity
- Cybersecurity insurance
- Cybersecurity research and development
- Cybersecurity workforce
- Federal governance
- Identity and access management
- International issues
- Internet of Things
- Public awareness and education
- State and local government cybersecurity

The Commission received more than 130 responses to the RFI from a wide range of respondents. Exactly 50 percent (65) of the respondents were from companies.⁴⁶ Just over 20 percent (26) of the respondents were trade and industry associations representing their members, which also are primarily from industry. Other institutions offered their insights in the RFI process, including individuals, nonprofits, sector coordinating councils, government agencies, and academic institutions. Organizations ranged from small businesses to international corporations, and from universities to standards-developing organizations.

All topics about which the Commission requested information were covered by the responses. Many respondents took the time to provide information on multiple topics. Critical infrastructure protection was the most commonly cited topic for Commission consideration, followed closely by federal cybersecurity governance.

The Commission reviewed and analyzed each of the RFI responses for content. More than 1100 unique recommendations were reviewed and considered. These recommendations ranged

from continuing current cybersecurity initiatives to radical shifts in approaches, including changes in direction for technology and research and development. The largest number of recommendations regarded federal cybersecurity governance (297, or 26 percent), followed closely by recommendations relating to research and development (222, or 22 percent).

45 "Information on Current and Future States of Cybersecurity in the Digital Economy," notice by NIST on August 10, 2016, Federal Register, <https://www.federalregister.gov/documents/2016/08/10/2016-18948/information-on-current-and-future-states-of-cybersecurity-in-the-digital-economy>.

46 All RFI responses are posted at <https://www.nist.gov/cybercommission/requests-information-rfis/rfi-responses>.

This page intentionally left blank.

Appendix 4: Executive Order 13718

This appendix provides the text of Executive Order 13718, “Commission on Enhancing National Cybersecurity,” February 9, 2016. The text is also available at <https://www.federalregister.gov/executive-order/13718>.

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to enhance cybersecurity awareness and protections at all levels of Government, business, and society, to protect privacy, to ensure public safety and economic and national security, and to empower Americans to take better control of their digital security, it is hereby ordered as follows:

Section 1. *Establishment.* There is established within the Department of Commerce the Commission on Enhancing National Cybersecurity (Commission).

Sec. 2. *Membership.* (a) The Commission shall be composed of not more than 12 members appointed by the President. The members of the Commission may include those with knowledge about or experience in cybersecurity, the digital economy, national security and law enforcement, corporate governance, risk management, information technology (IT), privacy, identity management, Internet governance and standards, government administration, digital and social media, communications, or any other area determined by the President to be of value to the Commission. The Speaker of the House of Representatives, the Minority Leader of the House of Representatives, the Majority Leader of the Senate, and the Minority Leader of the Senate are each invited to recommend one individual for membership on the Commission. No federally registered lobbyist or person presently otherwise employed by the Federal Government may serve on the Commission.

(b) The President shall designate one member of the Commission to serve as the Chair and one member of the Commission to serve as the Vice Chair.

Sec. 3. *Mission and Work.* The Commission will make detailed recommendations to strengthen cybersecurity in both the public and private sectors while protecting privacy, ensuring public safety and economic and national security, fostering discovery and development of new technical solutions, and bolstering partnerships

between Federal, State, and local government and the private sector in the development, promotion, and use of cybersecurity technologies, policies, and best practices. The Commission’s recommendations should address actions that can be taken over the next decade to accomplish these goals.

(a) In developing its recommendations, the Commission shall identify and study actions necessary to further improve cybersecurity awareness, risk management, and adoption of best practices throughout the private sector and at all levels of government. These areas of study may include methods to influence the way individuals and organizations perceive and use technology and approach cybersecurity as consumers and providers in the digital economy; demonstrate the nature and severity of cybersecurity threats, the importance of mitigation, and potential ways to manage and reduce the economic impacts of cyber risk; improve access to the knowledge needed to make informed cyber risk management decisions related to privacy, economic impact, and business continuity; and develop partnerships with industry, civil society, and international stakeholders. At a minimum, the Commission shall develop recommendations regarding:

(i) how best to bolster the protection of systems and data, including how to advance identity management, authentication, and cybersecurity of online identities, in light of technological developments and other trends;

(ii) ensuring that cybersecurity is a core element of the technologies associated with the Internet of Things and cloud computing, and that the policy and legal foundation for cybersecurity in the context of the Internet of Things is stable and adaptable;

(iii) further investments in research and development initiatives that can enhance cybersecurity;

(iv) increasing the quality, quantity, and level of expertise of the cybersecurity workforce in the Federal Government and private sector, including through education and training;

(v) improving broad-based education of

commonsense cybersecurity practices for the general public; and

(vi) any other issues that the President, through the Secretary of Commerce (Secretary), requests the Commission to consider.

(b) In developing its recommendations, the Commission shall also identify and study advances in technology, management, and IT service delivery that should be developed, widely adopted, or further tested throughout the private sector and at all levels of government, and in particular in the Federal Government and by critical infrastructure owners and operators. These areas of study may include cybersecurity technologies and other advances that are responsive to the rapidly evolving digital economy, and approaches to accelerating the introduction and use of emerging methods designed to enhance early detection, mitigation, and management of cyber risk in the security and privacy, and business and governance sectors. At a minimum, the Commission shall develop recommendations regarding:

(i) governance, procurement, and management processes for Federal civilian IT systems, applications, services, and infrastructure, including the following:

(A) a framework for identifying which IT services should be developed internally or shared across agencies, and for specific investment priorities for all such IT services;

(B) a framework to ensure that as Federal civilian agencies procure, modernize, or upgrade their IT systems, cybersecurity is incorporated into the process;

(C) a governance model for managing cybersecurity risk, enhancing resilience, and ensuring appropriate incident response and recovery in the operations of, and delivery of goods and services by, the Federal Government; and

(D) strategies to overcome barriers that make it difficult for the Federal Government to adopt and keep pace with industry best practices;

(ii) effective private sector and government

approaches to critical infrastructure protection in light of current and projected trends in cybersecurity threats and the connected nature of the United States economy;

(iii) steps State and local governments can take to enhance cybersecurity, and how the Federal Government can best support such steps; and

(iv) any other issues that the President, through the Secretary, requests the Commission to consider.

(c) To accomplish its mission, the Commission shall:

(i) reference and, as appropriate, build on successful existing cybersecurity policies, public-private partnerships, and other initiatives;

(ii) consult with cybersecurity, national security and law enforcement, privacy, management, technology, and digital economy experts in the public and private sectors;

(iii) seek input from those who have experienced significant cybersecurity incidents to understand lessons learned from these experiences, including identifying any barriers to awareness, risk management, and investment;

(iv) review reported information from the Office of Management and Budget regarding Federal information and information systems, including legacy systems, in order to assess critical Federal civilian IT infrastructures, governance, and management processes;

(v) review the impact of technological trends and market forces on existing cybersecurity policies and practices; and

(vi) examine other issues related to the Commission's mission that the Chair and Vice Chair agree are necessary and appropriate to the Commission's work.

(d) Where appropriate, the Commission may conduct original research, commission studies, and hold hearings to further examine particular issues.

(e) The Commission shall be advisory in nature and shall submit a final report to the President by December 1, 2016. This report shall be published on a public Web site along with any appropriate response from the President

within 45 days after it is provided to the President.

Sec. 4. Administration. (a) The Commission shall hold periodic meetings in public forums in an open and transparent environment.

(b) In carrying out its mission, the Commission shall be informed by, and shall strive to avoid duplicating, the efforts of other governmental entities.

(c) The Commission shall have a staff, headed by an Executive Director, which shall provide support for the functions of the Commission. The Secretary shall appoint the Executive Director, who shall be a full-time Federal employee, and the Commission's staff. The Executive Director may also serve as the Designated Federal Officer in accordance with the Federal Advisory Committee Act, as amended, 5 U.S.C. App. (FACA, the "Act").

(d) The Executive Director, in consultation with the Chair and Vice Chair, shall have the authority to create subcommittees as necessary to support the Commission's work and to examine particular areas of importance. These subcommittees must report their work to the Commission to inform its final recommendations.

(e) The Secretary will work with the heads of executive departments and agencies, to the extent permitted by law and consistent with their ongoing activities, to provide the Commission such information and cooperation as it may require for purposes of carrying out its mission.

Sec. 5. Termination. The Commission shall terminate within 15 days after it presents its final report to the President, unless extended by the President.

Sec. 6. General Provisions. (a) To the extent permitted by law, and subject to the availability of appropriations, the Secretary shall direct the Director of the National Institute of Standards and Technology to provide the Commission with such expertise, services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission.

(b) Insofar as FACA may apply to the Commission, any functions of the President under that Act, except for those in section 6 and section 14 of that Act, shall be performed by the Secretary.

(c) Members of the Commission shall serve without any compensation for their work on the Commission, but shall be allowed travel expenses, including per diem in lieu of subsistence, to the extent permitted by law for persons serving intermittently in the Government service (5 U.S.C. 5701-5707).

(d) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to a department, agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

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

THE WHITE HOUSE,
February 9, 2016.

This page intentionally left blank.

Appendix 5: Cybersecurity Policy Overview

This appendix provides an overview of selected cybersecurity policies established by recent administrations to address our nation's cybersecurity challenges.

Clinton Administration Policies

1. **Executive Order (EO) 13010, "Critical Infrastructure Protection,"** July 15, 1996.⁴⁷ EO 13010 established the President's Commission on Critical Infrastructure Protection, also known as the Marsh Commission. The purpose of this commission was to assess the vulnerabilities of critical infrastructures and develop recommendations for better protecting them.
2. **The Report of the President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructures,"** October 1997.⁴⁸ This report from the Marsh Commission concluded that our nation's critical infrastructure was facing increasing risks and that current defenses were minimal. The commission recommended a joint effort between the public and private sectors to improve security.
3. **Presidential Decision Directive 63 (PDD-63), "Critical Infrastructure Protection: Sector Coordinators,"** August 4, 1998.⁴⁹ Produced in response to the recommendations of the Marsh Commission, PDD-63 was the first U.S. policy statement on critical infrastructure, and it highlighted the need to better protect critical infrastructure from physical and cyber threats. PDD-63 was revoked and replaced by Homeland Security Presidential Directive 7 in 2003.
4. **"Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0,"** 2000.⁵⁰ This plan, which was created in support of PDD-63, proposed 10 programs to aid the federal government in protecting critical U.S. systems and networks. These programs include

identifying critical infrastructure assets and vulnerabilities, detecting attacks, sharing attack information, training security specialists, strengthening research and development efforts, and increasing public outreach.

Bush Administration Policies

5. **"The National Strategy to Secure Cyberspace,"** February 2003.⁵¹ This document provided a framework for ensuring that our nation's efforts to improve cybersecurity are effectively organized and prioritized. The strategy emphasized the need for a wide range of Americans to have roles in cybersecurity.
6. **Homeland Security Presidential Directive 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection,"** December 17, 2003.⁵² HSPD-7 changed federal agency responsibilities related to critical infrastructure protection. Its policy statements included designating an agency to lead protection activities for each critical infrastructure sector. HSPD-7 was revoked and replaced by Presidential Policy Directive 21 in 2013.
7. **"National Infrastructure Protection Plan" (NIPP),** 2006.⁵³ The NIPP was created to address requirements from HSPD-7. The NIPP defined the federal government's approach to identify "national priorities, goals, and requirements for CI . . . protection." Other information provided by the NIPP included the identification of federal agency responsibilities for critical infrastructure protection and the definition of the risk management framework to be used for assessing, prioritizing, and addressing risks to critical infrastructure.
8. **National Security Presidential Directive 54 (NSPD-54)/Homeland Security Presidential Directive 23 (HSPD-23), "Cybersecurity Policy,"** January 2008.⁵⁴ NSPD-54/

47 <https://www.gpo.gov/fdsys/pkg/FR-1996-07-17/pdf/96-18351.pdf>.

48 http://chnm.gmu.edu/cipdigitalarchive/files/5_CriticalFoundationsPCCIP.pdf.

49 <https://www.gpo.gov/fdsys/pkg/FR-1998-08-05/pdf/98-20865.pdf>.

50 https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/defending_americas_cyberspace_2000.pdf.

51 https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

52 <https://www.dhs.gov/homeland-security-presidential-directive-7>.

53 https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf.

54 This document is classified. Unclassified information about efforts resulting from this document is available at <https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>.

HSPD-23 started the Comprehensive National Cybersecurity Initiative (CNCI). The primary goals of the CNCI were “to establish a front line of defense against today’s immediate threats[,] . . . to defend against the full spectrum of threats[,] . . . [and] to strengthen the future cybersecurity environment.”

Obama Administration Policies

9. **NIPP 2009**, February 2009.⁵⁵ This document refined the original NIPP from 2006; its changes included adding critical manufacturing as a critical infrastructure sector and merging education into the government facilities sector.
10. **“Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,”** May 2009.⁵⁶ This report documented the results of a 60-day review of the federal government’s efforts regarding cybersecurity. It also made several recommendations, including the following:
 - “The Nation needs to develop the policies, processes, people, and technology required to mitigate cybersecurity-related risks.”
 - “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.”
 - “The government needs to increase investment in research that will help address cybersecurity vulnerabilities while also meeting our economic needs and national security requirements.”
11. **“National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy,”** April 2011.⁵⁷ The National Strategy for Trusted Identities in Cyberspace (NSTIC) was created to improve the security of online transactions by encouraging the private sector to develop tools for securing the identities of individuals and other entities involved in online transactions.
12. **“International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,”** May 2011.⁵⁸ This strategy complemented other Obama Administration cybersecurity policies by emphasizing the need for international cooperation to achieve technology reliability and security. Principles from the strategy include strengthening partnerships with a wide variety of stakeholders, implementing measures to dissuade and deter adversaries, and facilitating the development of global cybersecurity capabilities.
13. **Executive Order 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,”** October 7, 2011.⁵⁹ EO 13587 directed federal agencies to better protect the security of their classified information and, for such information involving people, to also protect the individuals’ privacy and civil liberties.
14. **Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,”** February 12, 2013.⁶⁰ EO 13636 initiated the development of a voluntary Cybersecurity Framework for organizations to use in reducing cyber risk to critical infrastructure. EO 13636 also directed the Department of Homeland Security (DHS) to produce a list of critical infrastructure systems and assets that could be disrupted by a cyber attack and directed federal agencies to notify private organizations if they were the target or victim of malicious cyber activity.

55 https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

56 https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

57 https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

58 https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

59 <https://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net>.

60 <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

15. **Presidential Policy Directive 21 (PPD-21), “Critical Infrastructure Security and Resilience,”** February 12, 2013.⁶¹ This directive recognized the importance of strengthening critical infrastructure security and resilience, and it recommended accomplishing such strengthening through collaboration among federal, state, local, tribal, and territorial government agencies, as well as public- and private-sector organizations. PPD-21 detailed federal agency roles and responsibilities related to critical infrastructure security and resilience, and it triggered several actions by these agencies in consequence.
16. **NIPP 2013,** December 2013.⁶² As directed by PPD-21, the 2009 version of the NIPP was revised and rereleased. The changes were much more extensive than those made in 2009 to the 2006 version. The 2013 version of the NIPP “reflects changes in the critical infrastructure risk, policy, and operating environments and is informed by the need to integrate the cyber, physical, and human elements of critical infrastructure in managing risk.”
17. **“Framework for Improving Critical Infrastructure Cybersecurity,”** February 2014.⁶³ Commonly known as the Cybersecurity Framework, this document “enables organizations —regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure.”
18. **Office of Management and Budget (OMB) M-15-01, “Fiscal Year 2014–2015 Guidance on Improving Federal Information Security and Privacy Management Practices,”** October 3, 2014.⁶⁴ This memorandum made several changes to federal cybersecurity practices, including a shift from periodic to continuous risk assessment and cybersecurity monitoring; it also authorized DHS to scan federal agencies’ publicly accessible networks for the presence of vulnerabilities.
19. **Executive Order 13691, “Promoting Private Sector Cybersecurity Information Sharing,”** February 13, 2015.⁶⁵ This EO promoted the creation of entities such as Information Sharing and Analysis Organizations (ISAOs) that enable businesses, government agencies, and other organizations to share cybersecurity information with each other.
20. **“FACT SHEET: Enhancing and Strengthening the Federal Government’s Cybersecurity,”** June 12, 2015.⁶⁶ This effort, better known as the 30-Day Cybersecurity Sprint, directed federal agencies to make several immediate improvements to their cybersecurity policies and processes. It also formed a Cybersecurity Sprint Team to review federal cybersecurity policies and processes, identify shortcomings and priorities, and recommend how to address them. In addition, the Sprint directed the development of a federal cybersecurity strategy based on the following key principles:
 - protecting data
 - improving situational awareness
 - increasing cybersecurity proficiency
 - increasing awareness
 - standardizing and automating processes
 - controlling, containing, and recovering from incidents
 - strengthening systems lifecycle security
 - reducing attack surfaces
21. **Office of Management and Budget M-16-04, “Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government,”** October 30, 2015.⁶⁷ The CSIP resulted from the 30-Day Cybersecurity Sprint. The CSIP established five objectives for federal civilian agencies:
 - a. “Prioritized Identification and Protection of high value information and assets;
 - b. “Timely Detection of and Rapid Response to cyber incidents;
 - c. “Rapid Recovery from incidents when they occur and Accelerated Adoption of lessons learned from the Sprint assessment;

61 <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

62 <https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf>.

63 <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.

64 <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf>.

65 <https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>.

66 https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/enhancing-strengthening-federal-government-cybersecurity.pdf.

67 <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf>.

- d. "Recruitment and Retention of the most highly-qualified Cybersecurity Workforce talent the Federal Government can bring to bear; and,
- e. "Efficient and Effective Acquisition and Deployment of Existing and Emerging Technology"
22. **"FACT SHEET: Cybersecurity National Action Plan,"** February 9, 2016.⁶⁸ This plan initiated several actions to improve cybersecurity for the federal government, the private sector, and individuals, including the following:
- Establish the Commission on Enhancing National Cybersecurity
 - Propose an IT modernization fund for the replacement of legacy technologies
 - Encourage users to adopt multifactor authentication
 - Propose a significant budget increase for federal cybersecurity efforts
23. **"Federal Cybersecurity Research and Development Strategic Plan,"** February 9, 2016.⁶⁹ The plan defined three cybersecurity R&D goals: (1) within the next 1 to 3 years, achieve the science and technology advances needed to "counter adversaries' asymmetrical advantages with effective and efficient risk management," meaning the ability to identify, assess, and respond to cybersecurity risks; (2) over the next 3 to 7 years, achieve advances to "reverse adversaries' asymmetrical advantages, through sustainably secure systems development and operation"; and (3) over the next 7 to 15 years, achieve advances "for effective and efficient deterrence of malicious cyber activities via denial of results and likely attribution."
24. **Executive Order 13718, "Commission on Enhancing National Cybersecurity,"** February 9, 2016.⁷⁰ This EO established the Commission that produced the present report. See Appendix 4 for a copy of EO 13718's text.
25. **Presidential Policy Directive 41, "United States Cyber Incident Coordination,"** July 26, 2016.⁷¹ PPD-41 clarified roles and responsibilities related to cybersecurity incident handling. It also directed the formation of a cyber unified coordination group (UCG) to coordinate incident response efforts for the most serious incidents.

Policy Themes

Common themes among these cybersecurity policies include the following:

- Improving the security of our nation's critical infrastructure
- Encouraging joint efforts involving a wide variety of public- and private-sector organizations to improve global cybersecurity;
- Improving federal cybersecurity policies and practices, especially in terms of incident response capabilities;
- Using risk management principles to assess vulnerabilities and select mitigations;
- Encouraging cybersecurity information sharing among public- and private-sector organizations;
- Increasing public awareness of cybersecurity; and
- Increasing investments in cybersecurity research.

Notably absent from these themes is regulation. Except for a brief period in the Obama Administration, the past three administrations have consistently eschewed regulation as a policy solution for cybersecurity.

Policy Criticisms

Fault has been found with the cybersecurity policies proposed by recent administrations, as well as with how those policies have been implemented. Here are examples of well-supported criticism from the past few years:

- In February 2013, the Government Accountability Office (GAO) released a report, GAO-13-187, titled "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented."⁷² It criticized federal cybersecurity strategy documents as follows:

68 <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>.

69 National Science and Technology Council, *Federal Cybersecurity Research and Development Strategic Plan: Ensuring Prosperity and National Security*, February 5, 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf.

70 <https://www.federalregister.gov/articles/2016/02/12/2016-03038/commission-on-enhancing-national-cybersecurity>.

71 <https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.

72 <http://www.gao.gov/assets/660/652170.pdf>.

“Although the federal strategy to address cybersecurity issues has been described in a number of documents, no integrated, overarching strategy has been developed that synthesizes these documents to provide a comprehensive description of the current strategy, including priority actions, responsibilities for performing them, and time frames for their completion. Existing strategy documents have not always addressed key elements of the desirable characteristics of a strategic approach. Among the items generally not included in cybersecurity strategy documents are mechanisms such as milestones and performance measures, cost and resource allocations, clear delineations of roles and responsibilities, and explanations of how the documents integrate with other national strategies. The items that have generally been missing are key to helping ensure that the vision and priorities outlined in the documents are effectively implemented. Without an overarching strategy that includes such mechanisms, the government is less able to determine the progress it has made in reaching its objectives and to hold key organizations accountable for carrying out planned activities.”

- December 2013 saw the release of “Liberty and Security in a Changing World: Report and Recommendations of the President’s Review Group on Intelligence and Communications Technologies.”⁷³ Regarding EO 13587, this report issued the following findings and recommendations:

“In recognition of the need to improve security on government networks with classified data, President Obama issued Executive Order 13587 to improve the security of classified networks against the Insider Threat. We have found that the implementation of that directive has been at best uneven and far too slow. Every day that it remains unimplemented, sensitive data, and therefore potentially lives, are at risk. Interagency implementation monitoring was not performed at a sufficiently high level in OMB or the NSS [national security staff]. The Administration did not direct the re-programming of adequate funds. Officials who were tardy in compliance were not held accountable. No central staff was created to enforce implementation or share best practices and lessons learned.”

We believe that the implementation of Executive Order 13578 should be greatly accelerated, that deadlines should be moved

up and enforced, and the adequate funding should be made available within agency budget ceilings and a Deputy Assistant to the President might be directed to enforce implementation. The interagency process might be co-led by the Deputy Director of OMB.

73 https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

This page intentionally left blank.

Appendix 6: Cybersecurity Legislation Overview

This appendix gives an overview of selected efforts by Congress to address cybersecurity.

1980–1989

1. **Public Law 98-473, “Counterfeit Access Device and Computer Fraud and Abuse Act of 1984,”** October 12, 1984.⁷⁴ This law made it illegal to access and use computers and computer networks without authorization to do so.
2. **Public Law 99-474, “Computer Fraud and Abuse Act of 1986,”** October 16, 1986.⁷⁵ Building on the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, this law made additional actions illegal, such as destruction of data without authorization and distribution of stolen passwords.
3. **Public Law 100-235, “Computer Security Act of 1987,”** January 8, 1988.⁷⁶ The Computer Security Act of 1987 was established to ensure that all federal agencies implemented basic cybersecurity measures for protecting sensitive information. The law designated the National Bureau of Standards (now known as the National Institute of Standards and Technology, or NIST) as the lead agency for developing cybersecurity standards, with the National Security Agency (NSA) providing assistance. This law was replaced by the Federal Information Security Management Act in 2002.

1990–1999

4. **Public Law 104-13, “Paperwork Reduction Act of 1995,”** May 25, 1995.⁷⁷ This law designated the Office of Management and Budget (OMB) as the agency responsible for federal agency cybersecurity policies.

5. **Divisions D and E, Public Law 104-106, “Clinger-Cohen Act of 1996,”** February 10, 1996.⁷⁸ The Clinger-Cohen Act designated agency responsibilities related to their cybersecurity policies and processes.
6. **Public Law 104-191, “Health Insurance Portability and Accountability Act of 1996,”** August 21, 1996.⁷⁹ The Health Insurance Portability and Accountability Act (HIPAA) included provisions for ensuring the security of sensitive health care information.
7. **Title II, Public Law 104-294, “National Information Infrastructure Protection Act,”** October 11, 1996.⁸⁰ Title II of this law revised the Computer Fraud and Abuse Act of 1986 by expanding the definitions of computer crime.
8. **Title V, Public Law 106-102, “Gramm-Leach-Bliley Act of 1999,”** November 12, 1999.⁸¹ This law required financial institutions to protect the confidentiality of all sensitive data regarding their customers.

2000–2009

9. **Public Law 107-204, “Sarbanes-Oxley Act of 2002,”** July 30, 2002.⁸² This law, directed at publicly owned U.S. companies, contained requirements to produce annual assessments of internal controls, including cybersecurity measures.
10. **Titles II and III, Public Law 107-296, “Homeland Security Act of 2002,”**⁸³ November 25, 2002. The Homeland Security Act established the Department of Homeland Security (DHS) to focus federal efforts on safeguarding the nation against threats, including cybersecurity threats, and to respond to disasters caused by these threats.

74 <https://www.gpo.gov/fdsys/pkg/STATUTE-98/pdf/STATUTE-98-Pg1837.pdf>.

75 <https://www.gpo.gov/fdsys/pkg/STATUTE-100/pdf/STATUTE-100-Pg1213.pdf>.

76 <https://www.gpo.gov/fdsys/pkg/STATUTE-101/pdf/STATUTE-101-Pg1724.pdf>.

77 <https://www.gpo.gov/fdsys/pkg/PLAW-104publ13/pdf/PLAW-104publ13.pdf>.

78 <https://www.gpo.gov/fdsys/pkg/PLAW-104publ106/pdf/PLAW-104publ106.pdf>.

79 <https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf>.

80 <https://www.gpo.gov/fdsys/pkg/PLAW-104publ294/pdf/PLAW-104publ294.pdf>.

81 <https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf>.

82 <https://www.gpo.gov/fdsys/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf>.

83 https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf.

11. **Public Law 107-305, “Cyber Security Research and Development Act,”** November 27, 2002.⁸⁴ The purpose of this law was to increase the federal government’s funding of cybersecurity research and development. Several ways to do so were specified, including:
 - National Science Foundation (NSF) research grants
 - Research fellowships awarded by NSF and NIST
 - The development of security configuration checklists by NIST to help agencies secure their computer hardware and software
 - The creation by NIST of the Computer System Security and Privacy Advisory Board, which was subsequently renamed the Information Security and Privacy Advisory Board (ISPAB)
 - A study by the National Academy of Science of critical infrastructure cybersecurity
 - Coordination of federal cybersecurity R&D efforts between NSF and NIST
12. **Title III—Information Security, Public Law 107-347, “The Federal Information Security Management Act of 2002,”** December 17, 2002 (also known as the “E-Government Act of 2002”).⁸⁵ The Federal Information Security Management Act of 2002 (FISMA) was intended to ensure that all federal agencies implemented basic cybersecurity measures at a minimum. FISMA designated NIST as the agency responsible for developing security guidelines and guidance to be used for securing federal civilian agency systems.
13. **Public Law 109-58, “Energy Policy Act of 2005,”** August 8, 2005.⁸⁶ This law required the Federal Energy Regulatory Commission (FERC) to develop standards for the reliability of certain types of electric power facilities.
14. **Public Law 109-295, “Department of Homeland Security Appropriations Act, 2007,”** October 4, 2006.⁸⁷ This law required new regulations for chemical facility security, including cybersecurity requirements.
15. **Public Law 110-140, “Energy Independence and Security Act of 2007,”** December 19, 2007.⁸⁸ This law designated NIST as the agency leading the effort to create interoperability standards for the smart grid.
16. **Division A, Title XIII and Division B, Title IV, Public Law 111-5, “Health Information Technology for Economic and Clinical Health Act,”** February 17, 2009.⁸⁹ This law built on HIPAA by requiring notifications for health care data breaches and strengthening penalties for insufficient protection of health care data.

2010–present

17. **Public Law 113-246, “Cybersecurity Workforce Assessment Act,”** December 18, 2014.⁹⁰ This law required regular assessments of the DHS cybersecurity workforce.
18. **Public Law 113-274, “Cybersecurity Enhancement Act of 2014,”** December 18, 2014.⁹¹ This law encouraged the public and private sectors to work together to improve cybersecurity in terms of research and development, workforce preparedness, and public awareness.
19. **Public Law 113-282, “National Cybersecurity Protection Act of 2014,”** December 18, 2014.⁹² The purpose of this law was to codify the responsibilities of the National Cybersecurity and Communications Integration Center (NCCIC).
20. **Public Law 113-283, “Federal Information Security Modernization Act of 2014,”** December 18, 2014.⁹³ This law modified FISMA to revise cybersecurity incident reporting requirements for federal agencies, clarify certain federal agency cybersecurity authorities, and streamline cybersecurity reporting.

84 <https://www.congress.gov/107/plaws/publ305/PLAW-107publ305.pdf>.

85 <https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>.

86 <https://www.congress.gov/109/plaws/publ58/PLAW-109publ58.pdf>.

87 <https://www.congress.gov/109/plaws/publ295/PLAW-109publ295.pdf>.

88 <https://www.gpo.gov/fdsys/pkg/PLAW-110publ140/pdf/PLAW-110publ140.pdf>.

89 <https://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf>.

90 <https://www.gpo.gov/fdsys/pkg/PLAW-113publ246/pdf/PLAW-113publ246.pdf>.

91 <https://www.congress.gov/113/plaws/publ274/PLAW-113publ274.pdf>.

92 <https://www.congress.gov/113/plaws/publ282/PLAW-113publ282.pdf>.

93 <https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf>.

21. **Public Law 113-291, “National Defense Authorization Act for Fiscal Year 2015,”** December 19, 2014.⁹⁴ Title VIII, Subtitle D of this law contains portions of what was originally H.R. 1232, “Federal Information Technology Acquisition Reform Act” (FITARA). The law required some changes to federal information technology practices that had implications for cybersecurity, most notably “consolidation of federal data centers.”
22. **Division N, Public Law 114-113, “Cybersecurity Act of 2015,”** December 18, 2015.⁹⁵ The Cybersecurity Act of 2015 contains the Cybersecurity Information Sharing Act (CISA). CISA encouraged the sharing of cybersecurity threat information among public- and private-sector organizations.

94 <https://www.congress.gov/113/plaws/publ291/PLAW-113publ291.pdf>.

95 <https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf>.

This page intentionally left blank.

Appendix 7: Acronym and Abbreviation List

| | |
|---------------|---|
| ABET | Accreditation Board for Engineering and Technology |
| ACM | Association for Computing Machinery |
| BLE | Bluetooth Low Energy |
| CEO | Chief Executive Officer |
| CFMWG | Cybersecurity Framework Metrics Working Group |
| CI | Critical Infrastructure |
| CIDAR | Cyber Incident Data and Analysis Repository |
| CIO | Chief Information Officer |
| CISA | Cybersecurity Information Sharing Act |
| CISO | Chief Information Security Officer |
| CNAP | Cybersecurity National Action Plan |
| CNCI | Comprehensive National Cybersecurity Initiative |
| CSIP | Cybersecurity Strategy and Implementation Plan |
| CSO | Chief Security Officer |
| CSRIC | Communications Security, Reliability and Interoperability Council |
| CTO | Chief Technology Officer |
| DARPA | Defense Advanced Research Projects Agency |
| DDoS | Distributed Denial-of-Service |
| DHS | Department of Homeland Security |
| DIUx | Defense Innovation Unit Experimental |
| DoD | Department of Defense |
| DOJ | Department of Justice |
| EO | Executive Order |
| ERM | Enterprise Risk Management |
| FACA | Federal Advisory Committee Act |
| FBI | Federal Bureau of Investigation |
| FBIIC | Financial Banking Information Infrastructure Committee |
| FERC | Federal Energy Regulatory Commission |
| FIDO | Fast IDentity Online |
| FISMA of 2002 | Federal Information Security Management Act of 2002 |
| FISMA of 2014 | Federal Information Security Modernization Act of 2014 |
| FITARA | Federal Information Technology Acquisition Reform Act |
| FOIA | Freedom of Information Act |
| FTC | Federal Trade Commission |
| GAO | Government Accountability Office |
| GPS | Global Positioning System |
| GSA | General Services Administration |
| HHS | Health and Human Services |
| HIPAA | Health Insurance Portability and Accountability Act |
| HSPD | Homeland Security Presidential Directive |
| IARPA | Intelligence Advanced Research Projects Activity |
| IC3 | Internet Crime Complaint Center |
| ICS-CERT | Industrial Control Systems Cyber Emergency Response Team |
| IEEE | Institute of Electrical and Electronics Engineers |
| IoT | Internet of Things |

| | |
|------------------|--|
| ISAO | Information Sharing and Analysis Organization |
| ISPAB | Information Security and Privacy Advisory Board |
| IT | Information Technology |
| ITMF | Information Technology Modernization Fund |
| MLAT | Mutual Legal Assistance Treaty |
| NCCIC | National Cybersecurity and Communications Integration Center |
| NCCoE | National Cybersecurity Center of Excellence |
| NCP ³ | National Cybersecurity Public–Private Program |
| NFC | Near-Field Communications |
| NHTSA | National Highway Traffic Safety Administration |
| NICE | National Initiative for Cybersecurity Education |
| NIPP | National Infrastructure Protection Plan |
| NIST | National Institute of Standards and Technology |
| NITRD | Networking and Information Technology Research and Development |
| NSA | National Security Agency |
| NSC | National Security Council |
| NSF | National Science Foundation |
| NSPD | National Security Presidential Directive |
| NSTAC | National Security Telecommunications Advisory Committee |
| NSTIC | National Strategy for Trusted Identities in Cyberspace |
| NTIA | National Telecommunications and Information Administration |
| OECD | Organization of Economic Co-operation and Development |
| OIRA | Office of Information and Regulatory Affairs |
| OMB | Office of Management and Budget |
| OPM | Office of Personnel Management |
| OSCE | Organization of Security Co-operation in Europe |
| OSTP | Office of Science and Technology Policy |
| OT | Operational Technology |
| PCII | Protected Critical Infrastructure Information |
| PDD | Presidential Decision Directive |
| PIV | Personal Identity Verification |
| PNT | Positioning, Navigation, and Timing |
| PPD | Presidential Policy Directive |
| R&D | Research and Development |
| RCO | Rapid Capabilities Office |
| RFI | Request for Information |
| RMF | Risk Management Framework |
| SBA | Small Business Administration |
| SES | Senior Executive Service |
| SLTT | State, Local, Tribal, and Territorial |
| SMB | Small and Medium-sized Business |
| SSA | Sector-Specific Agency |
| STEM | Science, Technology, Engineering, and Mathematics |
| UCG | Unified Coordination Group |
| URL | Uniform Resource Locator |
| U.S. | United States |
| USB | Universal Serial Bus |
| U.S.C. | United States Code |
| US-CERT | United States Computer Emergency Readiness Team |

Appendix 8: Glossary

Many of the definitions in this glossary are quoted or adapted from the following sources, which are listed here in order by their abbreviations:

- **40 U.S.C. § 1401** (1994): “Definitions.” <https://www.gpo.gov/fdsys/granule/USCODE-1998-title40/USCODE-1998-title40-chap25-sec1401>
- **40 U.S.C. § 11101** (2006): “Definitions.” <https://www.gpo.gov/fdsys/granule/USCODE-2011-title40/USCODE-2011-title40-subtitleIII-chap111-sec11101>
- **CNSSI 4009**: Committee on National Security Systems, “National Information Assurance (IA) Glossary,” CNSS Instruction No. 4009, April 26, 2010. <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>
- **FIPS PUB 200**: National Institute of Standards and Technology, “Minimum Security Requirements for Federal Information and Information Systems,” Federal Information Processing Standards Publication 200, March 2006. <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>
- **FIPS PUB 201**: National Institute of Standards and Technology, “Personal Identity Verification (PIV) of Federal Employees and Contractors,” Federal Information Processing Standards Publication 201-2, August 2013. <http://dx.doi.org/10.6028/NIST.FIPS.201-2>
- **Gartner OT**: “IT Glossary: Operational Technology (OT),” Gartner, <http://www.gartner.com/it-glossary/operational-technology-ot/>.
- **HSPD-23**: National Security Presidential Directive 54 (NSPD-54)/Homeland Security Presidential Directive 23 (HSPD-23), “Cybersecurity Policy,” January 2008.
- **IETF RFC 4949**: Robert W. Shirey, “Internet Security Glossary, Version 2,” Request for Comments: 4949, IETF, August, 2007. <https://tools.ietf.org/html/rfc4949>
- **ISO 9241-11**: International Organization for Standardization, “Ergonomic Requirements for Office Work for Visual Display Terminals (VDTs)—Part 11: Guidance on Usability,” ISO 9241-11:1998, March 19, 1998. http://www.iso.org/iso/catalogue_detail.htm?csnumber=16883
- **NIST CSF**: National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity,” Version 1.0, February 12, 2014. <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>
- **NIST SP 800-27**: Gary Stoneburner, Clark Hayden, and Alexis Feringa, “Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A,” NIST Special Publication 800-27 Rev A, June 2004. <http://dx.doi.org/10.6028/NIST.SP.800-27rA>
- **NIST SP 800-30**: Cybersecurity Framework: National Institute of Standards and Technology, “Guide for Conducting Risk Assessments,” NIST Special Publication 800-30, Revision 1, September 2012. <http://dx.doi.org/10.6028/NIST.SP.800-30r1>
- **NIST SP 800-37**: National Institute of Standards and Technology, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,” NIST Special Publication 800-37, Revision 1, February 2010 (includes updates as of 06-05-2014). <http://dx.doi.org/10.6028/NIST.SP.800-37r1>

- **NIST SP 800-39:** National Institute of Standards and Technology, “Managing Information Security Risk: Organization, Mission, and Information System View,” NIST Special Publication 800-39, March 2011. <http://dx.doi.org/10.6028/NIST.SP.800-39>
- **NIST SP 800-50:** Mark Wilson and Joan Hash, “Building an Information Technology Security Awareness and Training Program,” NIST Special Publication 800-50, October 2003. <http://dx.doi.org/10.6028/NIST.SP.800-50>
- **NIST SP 800-53:** National Institute of Standards and Technology, “Security and Privacy Controls for Federal Information Systems and Organizations,” NIST Special Publication 800-53, Revision 4, April 2013 (includes updates as of 01-22-2015). <http://dx.doi.org/10.6028/NIST.SP.800-53r4>
- **NIST SP 800-150:** Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, and Clem Skorupka, “Guide to Cyber Threat Information Sharing,” NIST Special Publication 800-150, October 2016. <http://dx.doi.org/10.6028/NIST.SP.800-150>
- **Patriot Act:** Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). <https://www.congress.gov/bill/107th-congress/house-bill/3162>
- **US-CERT ST06-001:** United States Computer Emergency Readiness Team, Security Tip (ST06-001), “Understanding Hidden Threats: Rootkits and Botnets,” August 24, 2011 (last revised February 6, 2013). <https://www.us-cert.gov/ncas/tips/ST06-001>

| | |
|-------------------------|---|
| adversary | See <i>attacker</i> . |
| assurance | The grounds for confidence that the set of intended security controls in an information system are effective. [adapted from NIST SP 800-27] |
| attack | Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. [CNSSI 4009] |
| attacker | An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. [NIST SP 800-30] |
| attribution | In the context of an attack or incident, identifying its source. In the context of information sharing, associating threat information with its source. |
| authentication | Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. [FIPS PUB 200] |
| awareness | Activities that seek to focus an individual’s attention on an (information security) issue or set of issues. [NIST SP 800-50] |
| botnet | A network of bots, which are compromised computers that an attacker controls remotely. Attackers use botnets to conduct denial-of-service attacks, distribute malware, and perform other tasks on their behalf. [US-CERT ST06-001] |
| critical infrastructure | Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. [Patriot Act] |
| cyber hygiene | The fundamental practices generally necessary to establish and maintain the security of any IT system. |

| | |
|---------------------------|---|
| cyber risk | Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. [NIST SP 800-37] |
| cyber risk management | The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. [NIST SP 800-39] |
| cybersecurity | The process of protecting information and information systems by preventing, detecting, and responding to unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [adapted from NIST SP 800-53 and NIST CSF] |
| cyberspace | The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers. [adapted from HSPD-23] |
| data breach | An incident that violates the confidentiality of data. |
| data manipulation | An incident that violates the integrity of data. |
| digital economy | The portion of the economy that relies directly on computer technology. |
| exploit | See <i>attack</i> . |
| identity | The set of physical, behavioral, and/or other characteristics by which an entity (human, device, service, etc.) is uniquely recognizable by an identity manager. [adapted from CNSSI 4009 and FIPS PUB 201] |
| identity management | Programs, processes, technologies, and personnel used to create trusted digital identity representations of humans, devices, services, and other entities; bind those identities to credentials that may serve as a proxy for the entities in access transactions; and employ the credentials to provide authorized access to resources. [adapted from CNSSI 4009] |
| incident | An occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [adapted from FIPS PUB 200] |
| industrial control system | An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems (SCADA) used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes. [NIST SP 800-53] |
| information sharing | The sharing of cybersecurity threat information with others, such as indicators (system artifacts or observables associated with an attack); tactics, techniques, and procedures (TTPs); security alerts; threat intelligence reports; and recommended security tool configurations. [adapted from NIST SP 800-150] |

| | |
|------------------------|--|
| information technology | Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. [adapted from 40 U.S.C. § 11101 and 40 U.S.C. § 1401] |
| intellectual property | Creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights. Under intellectual property law, the holder of one of these abstract “properties” has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered. [CNSSI 4009] |
| interdependency | The state in which two or more entities are reliant on each other. |
| Internet | The single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks. [adapted from IETF RFC 4949] |
| Internet of Things | Basically, connected sensors that can gather data by conducting physical analysis and (if capable) make changes to that physical environment. The Internet of Things is not just one product or even type of product, but rather a catalogue of technologies that are different than traditional information- and data-focused information technology. |
| legacy system | A system that uses software for which its vendor no longer corrects vulnerabilities. |
| malicious actor | See <i>attacker</i> . |
| operational technology | Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. [Gartner OT] |
| risk | A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [NIST SP 800-37] |
| secure coding | Following software development practices intended to reduce the number of vulnerabilities in the software. |
| threat | Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [NIST SP 800-30] |
| usability | The effectiveness, efficiency, and satisfaction with which the intended users can achieve their tasks in the intended context of product use. [ISO 9241-11] |
| vulnerability | Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [NIST SP 800-30] |

This page intentionally left blank.

This page intentionally left blank.
