# COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

## Meeting of the Commission on Enhancing National Cybersecurity

## PANELIST AND SPEAKER STATEMENTS

**American University**

Washington, DC

**September 19, 2016**

# Table of Contents

Dan Chenok 1
Evan Cooke 5
Alan Davidson 8
Karen Evans 12
Eric Fischer 14
Rick Geritz 20
Eric Mill 22
Chris Painter 25
Mark Ryland 28
Mike Walker 31
Gregory C. Wilshusen 32
Neal Ziring 40

## *Dan Chenok*

Good morning. I am Dan Chenok, Executive Director of the IBM Center for The Business of Government. The IBM Center connects research to practice, applying scholarship to real world issues and decisions for government. The Center facilitates discussion of new approaches to government effectiveness across multiple domains, including technology and cybersecurity.

I also serve as the Chair for the Cybersecurity Subcommittee of the DHS Data Privacy and Integrity Advisory Committee, as a member of the Center for Strategic and International Studies' Commission on Cybersecurity, and formerly served as Chair of the NIST Information Security and Privacy Advisory Board. In my Federal Government career, I served as Chief of the Information Policy and Technology Branch in the Office of Management and Budget (OMB). In addition to its budget role, OMB oversees multiple management functions across government; my office led work on information and IT policy and budget activity including cybersecurity.

I am very pleased to join you today to discuss the policy framework for Federal IT. I will provide brief perspectives on the evolution of Federal IT policies that impact cybersecurity, and then offer a few ideas as to what policy approaches might drive continued improvement for Federal IT and cybersecurity. I will focus primarily on civilian agency cybersecurity, which works under a different policy framework than is the case for national security systems.

### Background

The policy framework that governs Federal IT with respect to cybersecurity has many pieces. It is rooted in law, Executive Orders, OMB Circulars and Memoranda, NIST Guidance, DHS Directives, and other vehicles. Some major laws and policies are outlined below.

<u>Key Statutes</u>

- **Paperwork Reduction Act of 1980** – authorized OMB to oversee agency activity across a broad range of IT activities, and established the Office of Information and Regulatory Affairs (OIRA) to lead that effort. The PRA was in part a response to numerous reports of IT systems failures in the late 1970s, and established a framework for integrated IT oversight including privacy and security (the Privacy Act of 1974 was already under OMB's purview).
- **Computer Security Act of 1987** – gave the OMB Director authority over civilian agency computer security, with authority for national security systems delegated to the Secretary of Defense and Director of Central Intelligence. This division resulted after a debate over several years about whether oversight for civilian agency IT security should be led out of the intelligence community or by a civilian agency.
- **Clinger Cohen Act of 1996** – established Chief Information Officers in agencies to oversee information resources and IT management, including computer security. Clinger Cohen brought the emerging private sector best practice of a strategic CIO to government.
- **E-Government Act of 2002** – codified OMB's Office of E-Government and Information Technology (E-Gov), and charged the E-Gov Administrator with leadership for IT security, as well as overall IT and E-government leadership. The E-Gov Act came after years of discussion about the need for a Federal CIO or similar politically appointed IT leader at OMB, and contained provisions that codified multiple IT policies and practices including privacy. The leader of this office was designated as Federal CIO by this Administration.
- **Federal Information Security Management Act of 2002** (Title V of the E-Gov Act). FISMA updated the Computer Security Act. FISMA was reauthorized and updated in 2014 to enact provisions that drive agencies more toward operational security.
- **Federal Information Technology Reform Act of 2015** – enhanced authorities for Chief Information Officers to oversee IT activities, especially with respect to budget and acquisition. FITARA updated Clinger Cohen to give CIOs tools to control IT, following high-profile systems failures like healthcare.gov.

In addition to these general statutes, DHS' leadership for cybersecurity was authorized in the Homeland Security Act of 2002.

Key Policies

These statutes are implemented through a broad array of policy issuances. Several major policies follow, and agencies also must comply with a many additional guidance documents – among those are the policies governing Federal acquisition, which plays a key role in how IT and cybersecurity are implemented through contracts with private sector providers.

- **OMB Circular A-130** – OMB's overall policy directive that integrates Federal information and IT policy. A-130 was first issued in 1985 and revised since (with a recent update this summer); other OMB Circulars also have relevance for IT and cybersecurity, including the recent reissuance of Circular A-123 with its focus on Enterprise Risk Management (ERM).
- **OMB Circular A-11 Exhibit 55** – The annual requirement for agencies to report IT spending. The IT Budget became a separate exhibit under A-11, which is the overall annual budget guidance for agencies, in the late 1990s.
- **FISMA Guidance** – The annual requirement for agencies to report on security activities, issued each year since FISMA was implemented in 2004. FISMA guidance drives agency priorities and agency Inspector General reviews.
- **NIST Guidance** – For decades, NIST has issued multiple guidance documents on security, privacy, and identity management. These include binding Federal Information Processing Standards (FIPS), Special Publications that agencies leverage to make risk-based security decisions, and other non-binding documents (such as the 2014 NIST Cybersecurity Framework called for by Executive Order 13636).
- **Privacy Guidance** – OIRA works with the E-Gov Office on policy to implement the Privacy Act, Privacy Impact Assessments under the E-Gov Act, and other statues. In general, OIRA has the lead for privacy policy, while E-Gov has the lead for privacy in IT systems.
- **Identity Management Guidance** – For several decades, OMB has worked with NIST, GSA and DHS on various policies and programs regarding identity management, including:
    - Multiple GSA programs to implement electronic signatures and credentialing in government, starting in the 1990s and continuing today with the Federal Identity, Credential, and Access Management (FICAM) program;
    - the E-Authentication program led by OMB starting in 2001, now part of FICAM;
    - HSPD 12 issued in 2004, led by OMB and the White House and implemented in each agency for employee and contractor physical and logical credentialing; and
    - The National Strategy for Trusted Identities in Cyberspace (NSTIC), led by NIST and introduced in 2011, which calls for government to work with industry in developing identity management approaches that are secure, resilient, and privacy-protective.

Key Agencies

These laws and policies have led to a diverse set of lead cybersecurity organizations, including:

- the Cybersecurity Coordinator, housed in the National Security Council;
- the Office of Management and Budget, led by the Office of the Federal CIO -- in which a new position of Federal Chief Information Security Officer (CISO) oversees a Cyber Unit -- and also involving other OMB offices;
- the Department of Homeland Security, led by the National Protection and Programs Directorate (NPPD) and involving multiple additional DHS offices;
- the Commerce Department's National Institute of Standards and Technology (NIST);
- the General Services Administration, for authentication and cloud computing security;
- the Department of Justice for matters involving cyber crime;
- Agency Inspectors General, who conduct reviews under FISMA; and
- the Federal CIO Council, and specifically the Council's Information Security and Information Management Committee (ISIMC) whose members include agency CISOs.

**Perspectives on Enhancing Policy for Improved Federal Cybersecurity**

In a world where threats emerge in faster than policies and acquisitions can react to them, agility is essential. Policies can promote approaches and technologies through which government predict and prevent cyber threats. This Administration has taken important steps forward in developing and coordinating IT and cybersecurity policies, leveraging progress made in previous Administrations. Following are some ideas to continue enhancing this policy objective.

- **Rationalize governance around key priorities** – Agencies must manage their cyber assets under the broad policy and oversight structure described above. Clearly identifying roles and responsibilities, and focusing collective effort on key priorities for improving cyber in and across agencies, can have great benefit – especially for a new Administration that may need to take rapid action in response to a cyber incident. Developing a short set of key goals and objectives consistent with this structure, and making explicit responsibility and accountability for how these goals would be achieved and measured, would ensure that stakeholders in and with government would have a guidepost to align security actions. This need not be a long and detailed strategic plan – multiple cyber strategies already exist across the government. Rather, a new Administration could outline governmentwide priorities and lead organizations, a clear baseline architecture for technical protections across agencies, and pathways for deeper engagement with the private sector. Such a policy could be issued by the President via Executive Order or Directive to build on current progress. This approach would garner agency head attention, strengthening focus on cybersecurity across the government's C-Suite and stressing rapid action by mission leaders working with CIOs.
- **Drive innovation** – Given the multiple players, laws and policies that agencies must comply with, many cybersecurity resources necessarily go to compliance and reporting. There are relatively few incentives in the system to introduce innovation, making it difficult for government to tap into evolving commercial best practice. One path to address this concern could be through the procurement system. Most agency cybersecurity products and services are actually produced by industry through government contracts, under a set of complex rules that too often focus resources on inputs and tend to impede new ideas. Recent initiatives in government have attempted to leverage innovation by hiring outside technical talent, but cybersecurity expertise is not common in these initiatives; nor does this approach have much impact across the $90B spent on IT by the US government each year. Policies that can accelerate technology procurements will allow agencies to keep pace with innovation. And effective procurement requirements can incentivize sound cybersecurity practices, allowing companies to bring innovative ideas forward – such as how agencies can best leverage leading-edge commercial items, or harness the enormous potential of Blockchain -- as an expected contract activity. This could enable government to leverage the enormous IT investments to attract innovation, from companies that already carry out these investments through procurements.
- **Integrate security and privacy –** The recent reissuance of OMB Circular A-130 addressed privacy and security in a more coordinated fashion. Safeguarding personally identifiable information is a key element of cyber protection for government systems generally – yet teams across government that implement privacy are often organizationally separate from cybersecurity teams. More integration of policies, programs, and organizations can help align efforts around end goals for the protection of sensitive data that government holds in stewardship on behalf of its citizens. This integration can be reinforced by policies that call for agencies to account security and privacy spending.
- **Enhance Public-Private Collaboration** – In addition to leveraging innovation, policy can promote enhanced engagement across sectors to leverage best practice. Some ideas include:
  - Expand real-time threat information sharing at scale, building on the Cybersecurity Information Sharing Act of 2015;
  - Mature agency risk management programs to enable informed cyber choices, working with industry to understand the risk landscape relative to mission achievement by agencies – the NIST Cybersecurity Framework promotes such an approach, and integration of

government CIO and CFO responsibilities as part of an enterprise risk management would also benefit from adaptation of industry ERM models;

- Develop an approach to leverage commercial best practice for cybersecurity in government adoption of the Internet of Things; and
- Work with industry to speed the process for approving cloud-based cybersecurity under the FedRAMP program at GSA.

Thank you to the Commission for the opportunity to share these perspectives, and I look forward to the panel discussion.

## *Evan Cooke*

Good afternoon Chairman Donilon, Vice-Chairman Palmisano and Distinguished Members of the Commission. Thank you for the opportunity to participate in this discussion.

I'd like to start today by commending the Commission on exploring the topic of innovation in government and preparing for the future. As I hope our discussion this afternoon will highlight, there are ways to move fast in government, solve hard technical problems, and deliver meaningful change quickly. This past June, the White House published "100 Examples of President Obama's Leadership in Science, Technology, and Innovation" summarizing the capacity building efforts of this Administration to support innovation and transformation including the President's work creating three new high-level science, technology, and innovation positions in the White House—a U.S. Chief Information Officer, a U.S. Chief Technology Officer, and a Chief Data Scientist. These leaders have worked with colleagues to create the U.S. Digital Service, 18F at the General Services Administration (GSA), and the Presidential Innovation Fellows program—which have brought more than 450 engineers, designers, data scientists, and product managers who have signed on for a tour of duty to serve in over 25 agencies alongside dedicated civil servants to improve how government delivers modern digital services to the American people, and have further begun capacity building work to train existing federal technical talent. The President also reinvigorated the President's Council of Advisors on Science and Technology (PCAST). The background we discuss today will be on the U.S. Digital Service which will hopefully provide useful lessons and examples for your deliberations.

On August 11, 2014, the President directed his Administration to accelerate efforts to improve and simplify the digital experience between individuals, businesses, and the government through the creation of the U.S. Digital Service or USDS. Over the past two years, more than 170 engineers, designers, data scientists, and product managers have answered the President's call and signed on for a tour of duty with USDS. I was one of those engineers that dropped everything, moved across the country, and joined up.

Over the past two years this team has delivered more than 20 projects and initiatives. I'll touch quickly on three to give you sense for the work.

- **Making it easier for Veterans to access health care.** The Department of Veterans Affairs and U.S. Digital Service introduced a new digital application for health care upgrading a legacy application that 70 percent of visitors had trouble accessing. Following the launch of the new digital application, more than 10,000 Veterans used it to apply for health care, with many receiving coverage in less than 10 minutes.
- **Helping students, parents, and families make more informed decisions about college selection through the College Scorecard.** The Department of Education, 18F, and U.S. Digital Service launched the new College Scorecard tool to give students, parents, and their advisors the clearest, most accessible, and most reliable national data on college cost, graduation, debt, and post-college earnings. Within the first year, the College Scorecard had nearly 1.5 million users, more than 10 times the users its predecessor had in a year. In addition, by giving developers access to a developer application program interface (API), dozens of other organizations have used the Scorecard data to launch new tools to support students in their college search and application processes.
- **Strengthening information security at the Department of Defense (DoD).** The Defense Digital Service launched a program called Hack the Pentagon, the first bug bounty program in the history of the Federal Government, to strengthen the security of the DoD's digital assets. More than 1,400 outside researchers participated, and more than 250 submitted at least one vulnerability report. Of all the submissions received, 138 were determined to be legitimate, unique, and eligible for a bounty. These vulnerability reports were remediated in near-real time.

The U.S. Digital Service was created based on a simple theory of change: bring top technical talent into public service and deploy small empowered teams that partner with career civil servants and agency leadership to solve high-priority problems. USDS is organized as a federated set of connected but autonomous agency teams that work hand-in-hand with agency senior leadership using a variety of engagement models including two-week "discovery-sprints" to surface challenges, scope problems, and quickly deliver solutions. The concept of operations is best illustrated through the USDS core values.

- **Hire and empower great people** – Technology alone doesn't change things—it's the people who push our mission forward. Strong EQ (emotional quotient), compassion, and tenacity are just as important as being a great technologist.
- **Go where the work is** – By working shoulder to shoulder with agencies, we're able to inspire change. Transforming government is not up to the U.S. Digital Service. It's up to all of us, together.
- **Find the truth. Tell the truth** – We expect our people to be humble, not quiet, and challenge the status quo wherever data supports it. As has been said before, everyone is entitled to their own opinion, but not their own facts.
- **Design with users, not for them** – To deliver products and services that provide value to users, it's essential that we experience their experiences. The best products and services aren't created behind closed doors.
- **Optimize for results, not optics** – We work for the people—not credit, prestige, or headlines. This means tackling the hard stuff, even when success isn't guaranteed.
- **Create momentum** – The American people need better digital services, today. We work with a bias for action, focusing on delivery above all else.

Together, these values define a culture of delivery. That is, change is accomplished by focusing directly on results that improve the lives of citizens and customers.

This model has been successful in improving citizen-facing government services, a challenge that has several parallels to the problem of improving Federal cybersecurity. I share the following few thoughts as an implementer who has worked on U.S. Digital Service delivery teams and from a policy perspective in my current role in the Office of Science and Technology Policy.

Cybersecurity has an inherently technical basis and we won't have a full understanding of the issues we face or the available solutions unless we bring technical experience and understanding to our most senior discussions. We have observed time and time again how organizations cannot manage their way out of bad technical architectures. We need technologists at the table. One way in which USDS seeks to address this problem is by ensuring that position descriptions for job openings---even for senior roles---require a certain level of technical and operational experience. In addition, USDS works to ensure a diverse range of candidates that come from different backgrounds and experiences to enable a variety of problem solving approaches and perspectives.

The USDS model of bringing technical talent to do tours of duty in the Federal Government may also be a helpful tool in tackling important cybersecurity challenges. A few key features of the USDS model are the opportunity to work directly with senior agency leadership on critically important problems, the mandate to make difficult decisions that may challenge the status quo, and the autonomy to build and maintain a unique culture with leadership that is technical and has private-sector operational experience. These can be difficult requirements to realize but they have proved important components of success.

In addition to the engagement model and organizational structure our work on projects has also surfaced experiences that may be helpful data points for the Commission. First, many policies and processes designed with good intentions to improve cybersecurity in past years do not necessarily achieve the envisioned security outcomes. There is often limited evidence of measurable outcomes for many Federal cybersecurity policies and technologies. For example, rules put in place to strengthen the process of obtaining an authority to operate (ATO) can sometimes lead to inconsistent security outcomes, long review timelines, and significant duplication of effort across and even within agencies. Another example is Federal guidance to departments and agencies on Trusted Internet Connections, a policy that was originally put in place before the wide adoption of cloud and mobile technologies and that could be modernized to support new more secure tools.

Learning from these experiences, as we consider a more agile Federal policy framework for cybersecurity, compatibility with continually evolving technical architectures and accountability to real security outcomes may be helpful guidelines. Policy for cybersecurity should be tied to measurable results where possible and designed to evolve or sunset as technology matures.

Finally, our work has illustrated how difficult it is for a highly federated system to consistently implement a large number of complex changes quickly. The existing federated and distributed approach to agency IT and technology is becoming more difficult to manage and upgrade as the rate of change in technology increases. Consolidation of critical common services and platforms such as email and productivity applications will help provide the visibility and control necessary to position the federal government for a more automated world of advanced machine learning and artificial intelligence and defend against a next generation of threats.

Together, these lessons and experiences offer several opportunities including bringing more technical talent into senior cybersecurity roles, leveraging the USDS engagement model and structure where appropriate, upgrading Federal cybersecurity policy to be more accountable to results and designed to evolve as technology matures, and consolidation of critical common services and platforms such as email and productivity.

The U.S. Digital Service has shown us one model for change and innovation and also demonstrated an important point, *how* change can be achieved could be just as important as the question of *what* needs to be changed in an organization as large and complex as the Federal Government. There is no simple answer but empowering those who are close to the problem and understand the technology will get you a long ways.

Thank you for the opportunity to speak with you today.

## *Alan Davidson*

Good afternoon. I want to thank the Commission for inviting me to speak today, and for the tremendous effort that has been put into this undertaking already.

I would like to explore three key themes today for your consideration:

- **The digital economy is now a central feature of our broader economic prosperity.** The Internet and other digital technologies have in short order transformed the ability of people across the globe to access knowledge, to express themselves, to support social good, and to increase civic engagement. The digital economy is empowering future entrepreneurs and transforming existing industries. And it is still early: In many ways we have only just begun to realize the potential of the digital economy.
- **The digital economy will not thrive if people cannot trust their security online.** If we are to reap the benefits of an open and global digital economy in the future, we must work together to build trust for consumers, businesses, and government.
- **At the same time, any solutions we pursue must be consistent with our values and the strategic goals we are pursuing in the digital economy.** Around the world, bad actors are exploiting cyber security weaknesses for economic or political gain. The natural reaction from some will be to restrict access and seek control – an approach that alone could undermine the progress needed to build this trust and security. We need to get cybersecurity right, or risk undermining the open digital economy as a tool for social and economic good.

This testimony begins with a look at the opportunities and challenges offered by the digital economy today, and our strategic goals in pursuing them. Then we examine cybersecurity in that context.

### I. The Digital Economy: A Strategic Imperative

It is essential to understand cybersecurity in the broader context of our nation's strategic approach to the digital economy and Internet policy.

Our own work in this space at the Department of Commerce is driven by a conviction that the Internet and the broader digital economy are a critical part of the future success of the broader American economy. They are a source of jobs; an enabler of global trade; and a key element of U.S. competitiveness. They also enable people at home and around the world to access knowledge, build communities, and participate in civic life in unprecedented ways.

- Consider the ICT sector alone currently represents over 5 percent of GDP. In 2014, the U.S. exported $385 billion in potentially ICT-enabled services, imported $231 billion, and had a trade surplus of $154 billion for these Internet related services. Global data flows have been estimated to add $2.8 trillion to annual global GDP.
- Those numbers don't capture the digital economy's true impact or potential. Today, every company is a digital company. From web sites to back end systems to the Internet of Things, technology is changing how even main street businesses connect with consumers and run their companies. Experts estimate that this broader digitization has the potential to boost annual U.S. GDP up to $2.2 trillion by 2025. This would increase GDP by 6-8 percent above baseline projections.

This success is in many ways a function of the architecture of the modern digital economy. At its heart is the open, decentralized Internet. This gatekeeper-free network of networks has allowed innovation without permission, and access by anyone with a connection to information and global commerce. And it has allowed growth at scale – a digital economy today that encompasses millions of companies and organization, hundreds of millions of US consumers, billions of users worldwide, and now 10s of billions of connected devices.

But we cannot take this success for granted.

- Technology is changing rapidly. We anticipate continued growth in computing power, connectivity, and data usage along with developments such as artificial intelligence and the Internet of Things. These will impact the economic landscape (and directly impact cybersecurity.)
- U.S. business faces an intense competition globally. American leadership is not guaranteed.
- We have also seen the rise of new forms of regulation over the Internet – including data localization, limits on data flows, and proposals made in the name of privacy or security – that would undermine the open and global nature of the Digital Economy. Some of these policies are motivated by cultural differences, and some by heartfelt concerns about the need to protect consumers and business. But some raise serious questions about access to foreign markets. And some seem designed to undermine today's open exchange of information and commerce.

If the digital economy is to continue on its current course, we need to make the normative case to people around the world that a free and open Internet is good for them too – and that they will be safe and secure when they use it. We need to also ensure that our own policies – including our approach to security -- do not undermine our values or these key architectural features or give aid and comfort to those closed societies who would.

To address these grand challenges and opportunities, the Commerce Department has pursued a Digital Economy agenda based on four pillars.

- The first is protecting **cross-border data flows**, the lynchpin of the digital economy's success. The Department is working to promote a free and open global Internet, combat data localization, and promote multistakeholder Internet governance models.
- The second goal is **trust**. The digital economy will not succeed if people cannot trust their security and privacy online. In addition to its many efforts around cybersecurity, the Department is deeply engaged in privacy protection as well as ongoing conversations about government access to data.
- The third pillar is **access and skills**. American businesses need broadband infrastructure and a skilled workforce to compete. High-speed networks are essential to economic success in the 21st century. Yet, about a quarter of U.S. households still do not have Internet access at home.
- Our final pillar is **innovation**. This includes our work to promote smart intellectual property rules at home and abroad. We also want to engage with new technologies early in the development life cycle. This is often the best time to support new business opportunities and address long-term policy concerns.

The DOC is pursuing these digital economy initiatives in parallel with a variety of related work to promote use of government data, innovation, and economic measurement. We also partner closely with other agencies and the White House in promoting these goals. Overall, we are pursuing a policy approach to the digital economy that has evolved successfully over two decades. Its core tenets include openness, decentralization, technology neutrality, industry leadership, humility about regulation, and appreciation for global scope and scale. It is an approach has been embraced by consecutive Administrations since the 1997 Framework for Global Electronic Commerce, and enshrined in international documents such as the 2011 OECD Principles for Internet Policy-Making.

It is in this context that we need to consider our policy approach to cybersecurity and the digital economy.

## II. Cybersecurity to Promote the Global Digital Economy

As this Commission well knows, we face a growing national cybersecurity crisis, with broad implications. The string of high-profile attacks on popular brands and government institutions feed a narrative that undermines trust. And the global reactions, however well-intentioned, may ultimately threaten key features of our open digital economy, or be used by those who seek to control the flow of information and services.

Our great challenge is to address concerns about cybersecurity in a way that is consistent with our values and economic interests. If we do not address these concerns, we risk undermining the open, decentralized Internet.

We know that any comprehensive effort to improve cybersecurity will have many facets. There is no silver bullet that will fix our problems. But there are major areas of approach or initiative that could each make a substantial difference, and together could decisively improve security over time. While I am sure that at this point the Commission is familiar with much of this, let me commend to you a few areas worthy of your attention.

- **Risk-Based Approaches:** The Commerce Department – along with our partners across government – have focused on public-private partnerships and multistakeholder processes - working arm-in-arm with the private sector in programs that the Commission has heard quite a bit about, including the Cybersecurity Framework. In these approaches we take a framing that is removed from solely preventing any bad things from happening to an organization, towards a risk-based approach that considers how an organization can keep doing what it needs to do after a successful attack. Response and recovery capabilities are critical now.

  This approach also helps serve as a model for other countries, allowing them to also work to align their business' perspectives with their government needs – and preventing silos that threaten the growth of the Digital Economy.

- **Openness and Innovation** – The solutions we need will come from a free and open market, building on the power of our research and development infrastructure. The power in the digital infrastructure grew from a model of 'permission-less innovation,' where new ideas could be implemented and built up to scale without having to conform to existing expectations or top-down technical requirements. We will need this approach in the security world, to help identify new solutions, new uses of data, and new ways of looking at our existing systems to address evolving threats.
- **Private-Sector Engagement and Partnership**: As Secretary Pritzker has said, we still lack effective mechanisms for fostering meaningful government-industry cooperation across the full spectrum of cybersecurity issues. Only by working together can business and government reap the benefits of innovation and effective risk management.
- **Security By Design** – Building security into our systems, and integrating security thinking into the entire lifecycle of products and services is critical. 'Security by design' can sometimes feel like a hollow mantra. Everyone is for it, but even when there are successful, adaptable, scalable tools for building security in, we find their adoption slow. We need to find incentives and policies to help the market meet the demand for security.
- **Public Education** – Breaches and attacks dominate headlines, but more is needed to help technology users protect themselves. We need to foster greater awareness, and give both consumers and businesses the tools to understand and manage their risks. We have seen turning points in other public health and education campaigns – around seatbelts, littering, forest fires. What will be the turning point for cybersecurity-- where citizens begin to understand a personal connection? How do we help?
- **Harness New Developments to Drive the Market** – The Internet of Things and other developments offer a turning point to improve SME and consumer awareness of security issues and products – the stakes are higher. We can capture attention of the market and see additional innovation in this area, but government also has to incentivize private sector

players to collaborate on system-wide issues. And this is where public/private partnerships can fill the gap.

- **Building the Workforce -** We need a highly skilled and adaptive cybersecurity workforce to design, develop, implement, maintain, and continuously improve cybersecurity across the digital economy. We need to build on initiatives like the National Initiative for Cybersecurity Education (NICE), which as you know seeks to promote a cybersecurity workforce that matches the needs of businesses today, equips workers for 21st century careers, and keeps the United States on the leading edge of competitiveness worldwide. It is designed to foster and promote an ecosystem of cybersecurity education, training, and workforce development.

## III. Conclusion

In closing, we know progress in this area will be long and hard-fought. Improving cybersecurity will require us to look beyond point-in-time solutions and focus on developing a set of broad initiatives to stay ahead of an evolving threat in a very dynamic business and technical environment. To get it right will require the interplay of the right set of activities from both the public and private sectors.

I encourage you, as you think about your recommendations, to consider the broader context of digital economy policy-making that we are engaged in. We need to ensure that our own policies – including our approach to security – do not undermine our values, or give aid and comfort to those closed societies who would. If the digital economy is to continue on its current course, we need to make the case to people around the world that a free and open digital economy is good for all of us.

It is forums like these – where we openly discuss these issues – that gives us an advantage to establish the trust we need for this progress. Thank you for your time and attention today, and for your service.

## *Karen Evans*

Good Morning Chairman Donilon, Vice-Chairman Palmisano and Distinguished Members of the Commission. I am Karen Evans, the National Director of the US Cyber Challenge, which is a program within the Center for Internet Security, a not-for-profit organization. However, I am here today representing my previous role, Administrator for E-Government and Information Technology. This role is now known as the Chief Information Officer for US Government. I held this position for nearly six years during the George W. Bush Administration. Prior to this appointment, I was a career federal employee serving in multiple positions at various departments and agencies, culminating in my appointment into the Senior Executive Service (SES) as the Chief Information Officer (CIO) at the Department of Energy.

I would like to thank you for the opportunity to share with the Commission my views on the topic, "How did we get to here? The Policies that Shape Today's Federal IT Landscape."

As we are focusing on federal IT, I will limit my comments specifically to policies and/or legislation directly affecting the federal landscape. However, that said, there are other major legislative reforms that do need to be addressed that directly affect department and agencies such as data ownership.

Very early in my career, I managed the first hacking incident of the federal government at the Department of Justice which occurred August 1996. Since then, the landscape has changed, the threats are ever increasing, statutes and policies have been updated. I will focus my recommendations in three major areas: procurement, workforce and leadership with accountability.

1. **Procurement:** Agencies already have the tools they need to address cyber security gaps. Many analysts assert the federal procurement rules known as the Federal Acquisition Regulations (FAR) need to change. Conversely, I recommend federal department and agencies should actually enforce the terms and conditions of their contracts to produce better results. For example, the following is already required to be included in contracts:

   *All information technology acquisitions must meet the requirements outlined in the Federal Acquisition Regulation (FAR) Part 39.101 (d) policy ensuring the use of common security configuration checklists in the management of risk. National Institute of Standards and Technology (NIST) defines a security configuration checklist (also called a lockdown, hardening guide, or benchmark) as a document that contains instructions for securely configuring an IT product for an operational environment or verifying that an IT product has already been security configured. The National Checklist Program (NCP) that enables numerous Security Controls Action Program-validated security tools to automatically perform configuration checking using NCP checklists. Whenever feasible, organization should apply checklists to operating systems and applications to reduce the number of vulnerabilities that attackers can attempt to exploit and to lessen the potential impact of successful attacks.*

   This text begs the questions: how many agencies are actually using the NCP checklists and enforcing this provision? Are they using the tools developed? Are they requiring benchmarks? Are agencies effectively using the resources they already have?

2. **Workforce:** Agencies need leaders who have the skills to use the tools and produce desired results. The federal government has much work to do in improving skills and capabilities at many levels of the technology workforce. My efforts with the US Cyber Challenge are focused on increasing the numbers of qualified cybersecurity personnel who have the appropriate technical skills. We established the portal CyberCompEx.org (http://www.cybercompex.org), which serves as "social networking" site for individuals interested in pursuing cybersecurity positions as well as for employers. This work is a result of a joint effort between the federal

government (Department of Homeland Security, Science and Technology Directorate) and our private sector partners including SANS, Amazon Web Services and Monster.com.

However, I would like to specifically comment on the changing skills sets needed by CIOs. Many CIOs argue they don't "have a seat at the table." I would argue that "a seat at the table" is earned by having the skills and abilities to contribute to the agency's mission including protecting the agency from threats. I am hopeful this "excuse" will go away with the passage of the Federal Information Technology Reform Act (FITARA)[1] and with the update of the Federal Information Security Modernization Act (FISMA) of 2014[2]. The skills set needed by the CIOs includes more than just understanding policy. In my opinion, CIOs who have technical skills and understanding combined with the good communications and interpersonal skills will be successful. CIOs are the strategic advisers to the heads the Federal departments and agencies regarding the use and management of information while managing the risk associated with use of technology to provide the department and agency mission services. My recommendation to the Commission would be to urge rigorous enforcement of the requirement that CIOs possess BOTH the technical and policy skills to serve their agencies. Whether the CIO is political or career, the job description should be consistent with OMB assisting both the Office of Personnel Management and White House Presidential Personnel with the selections as envisioned by the Clinger-Cohen Act of 1996[3].

3. **Leadership with accountability**: We know what needs to be done. We have analyzed this challenge over and over again. The departments and agencies have plans upon plans with the most recent, Cybersecurity National Action Plan (CNAP). We need to execute of those plans. The excuses have been addressed: CIO authorities, FISMA updated, the Office of Management and Budget (OMB) Circular A-130 has been updated. We need the leadership and the will to get the hard work done. The leadership comes from Executive Office of the President and the appropriate organizations such as OMB and the National Security Council. Within the departments and agencies, the leadership needs to be the secretary or the head of the agency. The CIO supports the agency head but all the legislation is clear, it is the agency head who is responsible and accountable to the President. In the private sector, the CEO is responsible and accountable. The CEO has responsibility for all aspects including information technology, cybersecurity and the associated risks. It is necessary for the same to occur within the federal government.

Thank you again Mr. Chairman for allowing me to provide input into this process. I will continue assist your efforts as you may need. I am happy to answer questions you or the other members may have at this time.

[1] Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, P.L. No. 113-291

[2] P.L. No. 113-283

[3] Pub. L. No. 104-106, National Defense Authorization Act for Fiscal Year 1996.

## *Eric Fischer*

Chairman Donilon, Vice Chairman Palmisano, and distinguished Members of the President's Commission on Enhancing National Cybersecurity: Thank you for the opportunity to discuss with you today issues related to the role of federal information technology policies in shaping the cybersecurity landscape. My name is Eric Fischer, and I am the Senior Specialist in Science and Technology at the Congressional Research Service (CRS).

CRS is a legislative support agency for the U.S. Congress and is part of the Library of Congress. A major part of the mission of CRS is to provide Congress with nonpartisan, objective information and policy analysis on legislative issues. In keeping with that mission, CRS staff do not advocate for or take positions on policy. Consequently, this statement does not include any recommendations and should not be interpreted to reflect any association with recommendations made to or by the Commission.

The federal role in cybersecurity is complex, and that includes the role of legislation. No single overarching framework legislation is in place, but many enacted statutes—more than 50—address various aspects of cybersecurity. Some notable laws with provisions relating to federal information systems include these:

- The National Institute of Standards and Technology (NIST) Act (15 U.S.C. §271 et seq.), as originally enacted in 1901, created the National Bureau of Standards (renamed NIST in 1988) and gave it responsibilities relating to technical standards. Later amendments established a computer standards program and specified research topics, among them computer and telecommunication systems, including information security and control systems.
- The Brooks Automatic Data Processing Act (P.L. 89-306), enacted in 1965, gave the General Services Administration (GSA) authority over acquisition of automatic data processing equipment by federal agencies, and gave NIST responsibilities for developing standards and guidelines relating to automatic data processing and federal computer systems. It was repealed by the Clinger-Cohen Act of 1996.
- The Privacy Act of 1974 (P.L. 93-579) limited the disclosure of personal information held by federal agencies. It established a code of fair information practices for collection, management, and dissemination of records by agencies, including requirements for security and confidentiality of records.
- The Computer Security Act of 1987 (P.L. 100-235) required NIST to develop and the Secretary of Commerce to promulgate security standards and guidelines for federal computer systems except national security systems. The law also required agency planning and training in computer security (this provision was superseded by the Federal Information Security Management Act of 2002).
- The High Performance Computing Act of 1991 (P.L. 102-194) established a federal high-performance computing program and requires that it address security needs and provide for interagency coordination. Among its activities is production of an annual budget supplement on federal research and development (R&D) on networking and information technology, which has included cybersecurity as a program area since FY2007.
- The Paperwork Reduction Act of 1995 (P.L. 104-13) gave the Office of Management and Budget (OMB) authority to develop information-resource management policies and standards, required consultation with NIST and GSA on information technology (IT), and required agencies to implement processes relating to information security and privacy.
- The Clinger-Cohen Act of 1996 (P.L. 104-106) required agencies to ensure adequacy of information-security policies, OMB to oversee major IT acquisitions, and the Secretary of Commerce to promulgate compulsory federal computer standards based on those developed by NIST. It exempted national security systems from most provisions.

- The Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (P.L. 106-398) established an information assurance scholarship program in the Department of Defense (DOD). It also set cybersecurity requirements for federal systems, but was superseded by FISMA in 2002.
- The Federal Information Security Management Act (FISMA 2002, P.L. 107-296 and P.L. 107-347) created a cybersecurity framework for federal information systems, with an emphasis on risk management, and required implementation of agency-wide information security programs. It gave oversight responsibility to OMB, revised the responsibilities of the Secretary of Commerce and NIST for information-system standards, and required OMB to promulgate mandatory cybersecurity standards developed by NIST for federal systems. FISMA is arguably the statute with the broadest application specifically to the cybersecurity of federal civilian information systems.
- The Homeland Security Act of 2002 (P.L. 107-296) established the Department of Homeland Security (DHS) and transferred the Federal Computer Incident Response Center (now US-CERT) from GSA to DHS. In 2006, the Department of Homeland Security Appropriations Act (P.L 109-295) created the position of Assistant Secretary for Cybersecurity and Communications in DHS but did not specify responsibilities.
- The E-Government Act of 2002 (P.L. 107-347) guides federal IT management and initiatives to make information and services available online; established the Office of Electronic Government within OMB, the Chief Information Officers (CIO) Council, and a government/private-sector personnel exchange program; and contains various other requirements for security and protection of confidential information.
- The Cybersecurity Workforce Assessment Act (P.L. 113-246), enacted in 2014, required an assessment by DHS of its cybersecurity workforce and development of a workforce strategy.
- The Cybersecurity Enhancement Act of 2014 (P.L. 113-274) provided statutory authority for an existing NSF scholarship and recruitment program (called Scholarship for Service or Cybercorps) to build the federal cybersecurity workforce.
- The Border Patrol Agent Pay Reform Act of 2014 (P.L. 113-277) provided additional DHS hiring and compensation authorities and required a DHS assessment of workforce needs.
- The Federal Information Security Modernization Act (FISMA 2014, P.L. 113- 283) retained, with some amendments, most provisions of FISMA 2002. Changes include providing statutory authority to DHS for overseeing operational cybersecurity of federal civilian information systems, requiring agencies to implement DHS directives, and requiring OMB to establish procedures for notification and other responses to federal agency data breaches of personal information.
- The Cybersecurity Act of 2015 (P.L. 114-113) established in statute the DHS intrusion-protection program known as EINSTEIN, requires agencies to adopt it and implement additional cybersecurity measures, and gave DHS additional authority in the event of an imminent threat or emergency. It also facilitates public- and private-sector sharing of information on cyberthreats and defensive measures and requires the Office of Personnel Management (OPM) to establish and implement an employment-code structure for federal cybersecurity personnel.

The selection of laws described above are largely designed to address several well- established near-term needs in providing cybersecurity for federal systems, including agency responsibilities and programs, development and application of standards, information sharing, and workforce development. The gap in cybersecurity legislation between 2002 and 2014 illustrates the complexities and difficulties associated with legislating in this area. After enactment of FISMA 2002, Congress did not turn again to significant legislative activity in cybersecurity until 2009. Despite many calls and attempts to update FISMA, it was not successfully amended until the end of 2014. Similarly, attempts to pass laws to address longstanding issues such as information sharing were unsuccessful until the end of 2015.

The near-term needs exist in the context of more fundamental and difficult long-term policy challenges that, while they might be addressed in part through legislation, also arguably exacerbate the difficulties of enacting effective policy through legislation and other means in this area. The existence of such challenges has been recognized by various observers over many years. They can be characterized in many different ways. An approach that may be useful is to characterize a particular set that could be used to inform longer-term government and private-sector activities. One such set consists of four interdependent challenges: design, incentives, consensus, and environment (DICE). Legislation can potentially have an impact on all four, and some recently enacted statutes arguably affect aspects of them. While the challenges apply broadly across sectors, they have significant implications for the cybersecurity of federal systems.

**Design**. Experts often say that to be effective, security should be an integral part of hardware and software design, not something that is added on toward the end of the development cycle. Security that is added on is often criticized as being less effective and more cumbersome than security that is built in. Yet, traditionally, developers appear to have focused more on features other than security, largely for economic reasons. To the extent that investment in security is perceived to impede investment in other features or to extend the time required to develop a new product or service, it may not be regarded as cost-effective. Also, security risks that may arise in the future can seldom be predicted with certainty, posing a difficult challenge for designers.

Harmonizing security with usability is also part of this challenge. If cyberspace has not been designed with security in mind, it can also be said that security has not been designed with usability in mind. Poor usability can make security much less effective. As the recent debate over passwords has illustrated, users will often find ways to work around usability problems with security features, even if such workarounds compromise the effectiveness of those security measures—for example, by using the same password for different purposes or recording passwords in ways that could be accessed by others. Investments in education and awareness seem unlikely to be sufficient by themselves to solve that problem. Educating people about the importance of good password security does not solve the usability problem.

What can be done legislatively about the design challenge? One option is through federal investment in R&D. The Commission might wish to ask if the current degree of emphasis on design R&D, including usability, is sufficient to meet this challenge, or whether federal research priorities need to be revised. Another option would be to determine if security is a sufficiently integral part of the education and training of IT engineers and programmers at present, or if curricula need to be revised to ensure that those receiving degrees understand the importance of cybersecurity and how to implement it in system design.

A third option is to examine how the federal government, as one of the largest users of IT products and services in the world, can use its acquisition leverage more extensively to advance development and implementation of cybersecurity. (While the term IT is used in this statement, the original IT industry has also increasingly converged with the communications industry into a combined sector commonly called information and communications technology, or ICT, to which many of the points made in this statement may also apply.) For example, EPEAT is a green electronics label based on a recognized multifactor technical standard (IEEE Standard 1680). It was developed by a private, nonprofit organization with partial funding from the Environmental Protection Agency (EPA). Executive Orders 13423 (Strengthening Federal Environmental, Energy, and Transportation Management) and 13514 (Federal Leadership in Environmental, Energy, and Economic Performance) require agencies to acquire EPEAT-labelled electronic products, if available, in most instances (48 C.F.R. 23.704). EPA also developed the Federal Electronics Challenge (FEC), a partnership aimed at facilitating green practices in purchase, use, and disposal of electronics. Such examples of multifactor approaches to complex issues might be worth examining for their potential applicability to improving the cybersecurity of federal information systems.

**Incentives**. The structure of economic incentives for cybersecurity has been called distorted or even perverse. Cybercrime has long been regarded by many observers as cheap, profitable, and comparatively safe for the perpetrators. In contrast, cybersecurity can be expensive, is by its nature imperfect, and the economic returns on investments are often unsure. A key question is, how does one increase the net cost of cybercrime and make cybersecurity more effective and affordable? There are various potential ways that both of those goals can be approached, such as increasing penalties for cybercrime, improvements in system and process design, and development of the cybersecurity insurance market.

An additional consideration is the degree to which users demand good cybersecurity as an essential feature of IT systems and services. It can be argued that this problem will persist until users treat good cybersecurity as an essential part of the value proposition when considering the acquisition of goods and services. So the question becomes, how does one shift the demand curve for cybersecurity in the desired direction? Changes in consumer attitudes about automobile safety illustrate that such shifting is possible. In the 1950s, consumers did not respond well to attempts by manufacturers to advertise the safety features of their vehicles. A variety of factors, including campaigns by activist groups, media attention, technology innovations, and federal and state legislation setting safety standards and driver requirements, among others, led over the following decades to a shift in consumer demand for safety features, which are now commonly promoted in automobile advertising campaigns.

The demand curve for cybersecurity varies among sectors. For the government sector, with its inherently monopolistic features and powers of compulsion, trust is an important expectation for consumers, so the demand for security should arguably be much higher than for many other sectors. From that perspective, one can argue that government should be a leader in ensuring the cybersecurity of its information infrastructure. That does not, however, appear to be a widely held view at present among observers. A question for the Commission may be what should the federal goal be with respect to national and even global leadership in cybersecurity of federal information systems, and how can it be achieved? Similar arguments can be applied to nonfederal government systems.

**Consensus**. Cybersecurity means different things to different stakeholders. There are often disagreements on its meaning, implementation, and risks. Substantial cultural impediments to consensus also exist, not only between sectors but within sectors and even within organizations. Efforts such as the development of the NIST-led cybersecurity framework appear to be achieving some improvements in such consensus. One option for addressing this challenge would be to build on the NIST effort. It might also be possible to use the standards-development effort established for information sharing and analysis organizations by Executive Order 13691 (Promoting Private Sector Cybersecurity Information Sharing) as a lever for building consensus within and across sectors.

There is also a fundamental conceptual problem that may impede the development of a useful consensus. The increasing economic and societal prominence and growth of cyberspace arises to a significant degree from its ability to connect things and apply computing power to them in unprecedented and useful ways. In contrast, security traditionally involves keeping things apart by isolating protected assets from potential threats. That arguably creates a fundamental conflict with respect to how the need for security can be reconciled with the benefits of connectivity in cyberspace. Increasingly, cybersecurity experts and other observers are arguing that traditional approaches such as perimeter defense are insufficient, but consensus on a new conceptual framework has yet to emerge. One option for the Commission would be to determine if R&D and other efforts should be accelerated to develop such a new framework.

The consensus challenge is complex, and an essential step in resolving it is likely to be identifying the key areas where consensus is lacking. It might be worth considering whether more effort should be given to expressly identifying those areas, and what can be done to resolve those differences. Efforts such as the NIST framework might serve as useful models to consider.

**Environment**. Cyberspace has been called the fastest evolving technology space in human history, both in scale and properties. This rapid evolution poses significant challenges for cybersecurity, exacerbating the speed of the "arms race" between attackers and defenders, and arguably providing a significant advantage to the former. New and emerging properties and applications—especially social media, mobile computing, big data, cloud computing, and the Internet of Things—further complicate the evolving threat environment, but they can also pose potential opportunities for improving cybersecurity, for example through the economies of scale provided by cloud computing and big data analytics. In a sense, such developments may provide defenders with opportunities to shape the evolution of cyberspace toward a state of greater security. However, any such attempts would presumably need to take into account the inertia created by the substantial presence of legacy systems. That has been cited as a problem in particular for federal IT.

At the same time that cyberspace is evolving so rapidly, there are core components that are highly conserved. For example, the fundamental model used for Internet communications has been in use for decades.

Such a combination of observed and evolved features is analogous in some ways to the evolution of biological organisms. As the geneticist Francois Jacob pointed out many years ago, the evolutionary process acts more like a tinkerer than an engineer. As a species evolves, new features often evolve from old ones (a classic example is the historical relationship between the gill arches of fishes and the bones of the human middle ear), and even new ones can only function effectively in conjunction with existing components. While it is easy to take such analogies too far, it may be useful to point out that attempts to shape the evolution of cyberspace toward greater cybersecurity need to consider the whole cyberspace "organism," not just individual components.

The continuing evolution of cyberspace also implies that it is not yet a mature technology space. That characteristic creates uncertainties that can affect the ability of governments to create stable and effective policies and suggests that attempting to apply policy approaches designed for stable and mature technologies may not be optimal.

**Election Security**. Cybersecurity as applied to the administration of federal elections is an example that, while it does not directly involve federal IT, illustrates the role of all four challenges. It might be considered a special case, given the role of state governments in running elections, but it is an issue of national concern, and it may not be as atypical as it appears, given that most of the components of the nation's critical infrastructure are owned and operated by the private sector.

The security of computer technology used in elections has reemerged this year as a significant issue. It has long been argued that electronic voting systems have not been designed with adequate consideration of security. The federal requirements in the Help America Vote Act of 2002 brought new focus to this issue by facilitating the use of voting systems by states that record votes directly to a computer memory. When experts and advocates raised concerns about the risks posed by attempts to tamper with such systems, a common response by election officials was to add security layers, which in many cases decreased usability.

Addressing those issues is difficult in part because the voting system market is fragmented and episodic, with a fixed customer base. Those features can create significant barriers for entry into the market by entrepreneurs and reduce incentives for innovation. The short-term funding that HAVA provided in FY2003 and FY2004 helped states replace antiquated equipment, but it did not appear to stimulate much innovation, with a few exceptions such as the development of electronic pollbooks. Even with the attention paid to security after the enactment of HAVA, there is a lack of consensus overall about the security of our election system. Some observers express concerns that cyberattacks on voting systems could affect vote counts and that attacks on registration systems could disrupt voting or prevent legitimate voters from casting ballots. Others argue that the decentralization and diversity of the national election infrastructure, along with the range of security measures that state and local election officials have already implemented, poses sufficient barriers to prevent a coordinated attack from having significant impact.

Concerns have been exacerbated both by the increased use of IT by state and local election offices—stimulated in part by another HAVA requirement for computerized statewide voter registration lists. The threat environment has also changed, as demonstrated by evidence of attempted interference by nation-states through cyber- intrusions. While elections are run by states, the federal government plays an important role, especially through HAVA, and it might be worthwhile to consider how a consensus can be reached on whether the federal role should change given the current and anticipated threat environment.

## *Rick Geritz*

The shortage of cybersecurity talent has become one of the most visible and pressing issues in the United States as cybers impacts every aspect of the economy from finance, energy and healthcare, to telecommunications and critical infrastructure. This has a direct impact on our nation's ability to create the cybersecurity skills needed to protect our country and innovate our future.

Meeting this challenge in a sustainable way must begin with education.

High schools and universities are being challenged to introduce cybersecurity to the nation's next generation in order to create a substantial pipeline of inspired "cyber students". The reality is that high schools and teachers lack cyber security skills and training. Cybersecurity is the modern equivalent of the space race. The need for cyber security already impacts culture and education in much the same way the space race did. Technology is the new alphabet and the foundation for digital opportunities.

Policy makers are focused on the imperative to create the "cyber generation," as so presciently started by the Obama Administration, which is continuing to make cyber education a priority on a nationwide basis. This is being done with the creation and full support of the National Initiative for Cybersecurity Education (NICE), the National Science Foundation (NSF) and DoC ... and by appointing a Commission that relies primarily on private sector expertise to address the important questions of what has to be done to improve and ensure our collective cybersecurity.

Policy makers seek platforms which operate as accelerators and force multipliers for students to test drive cyber security career options through scalable mentorship programs. Evidence[4] informs us that mentoring is critical -- to both students and teachers -- to imparting up-to-date knowledge about the field, the marketplace needs, and career opportunities. These platforms must be designed to facilitate the spirit of collaboration among all participants committed to the universal goal--to optimise the national, and ultimately the planetary human capital base.

Our task is to:

- make cybersecurity relatable for students so they are eager to learn;
- showcase the rewarding and in demand careers in cybersecurity; and
- improve the knowledge and capability of educators in order to inspire students to become part of America's digital economy.

We herewith submit recommendations that would positively impact America's pipeline of qualified students -- the Next Cyber Generation -- entering our workforce:

(1) A "Day of Cyber " exposure of cybersecurity skills to all students so they understand the opportunity;

(2) An at-scale mentoring system that taps into industry's current experts and specialists;

(3) Cybersecurity training for all teachers in the nation, irrespective of background or current course/teaching assignments; and

(4) A nationwide cybersecurity informational and promotional framework for university use in attracting and motivating students to enter, and remain in cybersecurity programs.

[4] 2008 study by NIH: Does Mentoring Matter? A Multidisciplinary Meta-Analysis Comparing Mentored and Non-Mentored Individuals. Lillian T. Eby , Tammy D. Allen , Sarah C. Evans , Thomas Ng , and David DuBois. Our findings are generally consistent with previous reviews focusing on a specific type of mentoring (youth, academic, workplace). Both Allen et al. (2004) and Underhill (2006) found significant relationships between workplace mentoring and career attitudes, work attitudes, and some career outcomes. Reviews of youth ( DuBois et al., 2002 ) and academic ( Sambunjak et al., 2006 ) mentoring found an association between mentoring and both career and employment outcomes.

Thank you Mr. Chairman, for allowing me to contribute to this important process. We remain committed to assisting further as needed. I'm happy to answer any questions that you or other members might have at this time.

## *Eric Mill*

Thank you to Chairman Donilon, Vice Chairman Palmisano, and the other distinguished members of the Commission for inviting me to appear here today.

I work at the General Services Administration, where I have served as a policy advisor for GSA's Technology Transformation Service and a software engineer on its 18F team. My comments today are my own, and do not necessarily represent the entirety of GSA, but I hope that they can offer the Commission some practical perspective.

My work at GSA includes a strong focus on information security policy and practice in the federal government. This means not only developing policies that improve federal information security, but developing new software tools to support policy implementation, and working directly with agencies to identify and resolve technical issues.

Today, I want to share a few suggestions from my work in the federal government. They are each simple in concept, but also challenge core assumptions and operations in federal agencies.[5]

**First**, federal agencies must recruit and elevate active technical practitioners within their organization. Employing staff with active technical skills is absolutely necessary in order for agencies to control fundamental aspects of their information security posture.

This means hiring engineers, penetration testers, and other technical specialists to perform technical functions in-house. Today, this is something that many federal agencies -- even agency IT offices -- often simply do not do. Instead, many agencies largely outsource technical analysis, engineering, and deployment tasks. The growth of "digital services" teams in federal agencies has made a positive impact on bringing technologists into government, but these teams are not usually tasked with performing key agency IT management or information security functions.

However, simply hiring technical specialists is not enough. For the public service to get the most value from its technical staff, and for its technical staff to get the most value from their public service, practitioners must have the autonomy to set agency strategy and to implement modern solutions, and must be given a voice on agency-wide and government-wide decisions.

This requires agencies to make real investments in their technical staff, and for their formal hierarchy to contemplate placing practitioners in senior positions with broad mandates to directly improve agency IT and information security, without necessarily requiring these positions to be supervisory. It also requires that agencies integrate their technical staff into internal and government policy-making processes. Just as agencies call upon their legal staff to provide more than rote analyses of legal risk, agencies should become accustomed to relying on their technical staff when making strategic decisions.

**Second**, the federal government must drastically change its approach to information sharing. Overwhelmingly, federal agencies default to severe restrictions on sharing documentation, policies, data, and software with the public -- and, in effect, with other agencies.

The federal government is terrifically large, and effecting real change is not always possible through top-down policies and chain-of-command coordination alone. To change how the federal government operates, it is necessary to share information and technology in the widest and most organic ways possible. In practice, the most effective way, by far, for information to have government-wide impact is for it to be distributed publicly.

[5] These recommendations also apply to policy-making and oversight bodies, such as executive offices, legislative agencies, and offices of inspectors general.

In its comments to the White House on its then-proposed source code policy, 18F described this problem as it relates to software code2 (emphasis added):[6]

> We have consistently seen that the most effective way to share information, software, and experience among agencies is the ongoing public release of data, code, and documentation. Managing and guarding access to "private" software and information consistently entails significant operational overhead when compared to sharing public information. The bureaucratic overhead of secrecy can sometimes be extreme, depending on the scale and temperament of the collaborators. However, this overhead is frequently discounted or unobserved by teams that default to working in private.

Source code is just one example. Agencies can share their technology and security practices without releasing sensitive information. This includes releasing software documentation, sharing agency-wide security policies, publishing technical blog posts, and speaking at conferences about internal practices. As part of this, agencies should become comfortable speaking about their failures and incidents, and how they responded and learned from them. These are some of the critical mechanics that allow the technology industry to rapidly evolve and to have its lessons and best practices spread throughout its community of practice.

This will require greater trust between agency communications and legislative affairs teams and other agency components. Oversight bodies, such as inspector general offices and congressional committees, should encourage this information sharing and should work collaboratively with agencies to resolve security incidents and internalize their lessons.

This may be an uncomfortable transition for some agencies at first. However, if the federal government's security practices are to keep pace with a changing world, this must become the norm for the federal government.

**Third**, federal agencies need to be reducing their dependence on their network "perimeter", and to avoid unnecessarily centralizing their resources.

Increasingly, maintaining and relying on a trusted network -- whether for a single agency or for multiple agencies -- is in stark conflict with broader trends in the technology industry and the information security community. This conflict can create major inefficiencies in government operations, as well as misalignment of security resources.

The most obvious conflict is that the federal government is under strong practical, policy, and economic pressures to move to "the cloud" -- that is, to rely on computing resources that are beyond their direct control. The benefits of commercial cloud services are numerous, but their use requires placing trust in third parties. These cloud services themselves often have many of their own business relationships with other cloud service providers. Trust is managed through legal agreements, and through software and security mechanisms that limit the amount of trust that needs to be placed in connected third parties. This trend moves agency resources out of agency-controlled locations, while making it easier to support a mobile federal workforce that can access agency resources from any network. This makes reliance on a perimeter increasingly less necessary and less worthwhile.

There is also a clear trend in the information security community towards assuming that components will suffer compromises, relying on privilege separation to limit the effect of compromise, and generally avoiding large central points of failure. Unfortunately, there is a strong tendency in the federal government to centralize resources, such as by creating small numbers of entry and exit points in networks. Limiting the number of network entry points in this way, while conceptually straightforward, places unrealistic security expectations on those entry points. These can lead to

[6] https://github.com/WhiteHouse/source-code-policy/issues/73, "Open source by default". A public comment by 18F on what eventually became https://sourcecode.cio.gov.

unrealistic security models inside federal agencies, leading staff to rely too heavily on a “trusted network” and failing to require proper privilege separation.

Fundamentally, the path forward for technology and security to scale in the modern world is to rely on logical barriers (software) rather than physical barriers (the perimeter). This means that agencies should broadly be moving away from intranets, and investing in software-based solutions to privilege management.

These recommendations describe a public service that is:

- Supported by a community of technical practitioners with the mandate and ability to make their agencies leaders in information security,
- Accelerating its collective progress by routinely and publicly sharing the work of its staff among the federal community, and
- Has the technical skills to build a modern decentralized infrastructure based on realistic threat models and an embrace of contemporary security trends.

I believe that the above captures how today’s most successful technology organizations function, and describes a federal government that can take care of itself.

Thank you again for the opportunity to comment, and for the Commission’s important work on improving our nation’s security.

## *Chris Painter*

Chairman Donilon, Vice Chairman Palmisano, and members of the Presidential Commission on Enhancing National Cybersecurity, thank you for the opportunity to speak to you.

Through its diplomacy, the State Department works energetically to strengthen our collective cybersecurity. Our efforts to coordinate, consult, and negotiate with a range of countries and international organizations complement the practical, day-to-day work of our interagency colleagues who maintain network security. Our cyber diplomats work to reduce risk and enhance stability in cyberspace. These efforts include but are not limited to working with our interagency partners to promote internationally a framework for cyber stability; building the capacity of foreign governments to promote cybersecurity and respond to cyber threats; using diplomatic channels to support cyber incident response; and partnering with other countries to combat transnational cybercrime and promote membership in the Budapest Convention. In each of these areas, we take care to ensure that our policy recommendations, capacity building efforts, and foreign assistance programs respect and reinforce the rule of law, the free flow of data, and human rights, including freedom of expression. I will discuss each of these lines of effort and offer a few policy recommendations.

### Enhancing a Framework for International Stability in Cyberspace

To strengthen cybersecurity on the international level, the Department of State, working with our interagency partners, is guided by the President's 2011 *International Strategy for Cyberspace*, which sets out a strategic framework of international cyber stability designed to achieve and maintain a peaceful cyberspace where all states are able to fully realize its benefits, where there are advantages to cooperating against common threats and avoiding conflict, and where there is little incentive for states to engage in disruptive behavior or to attack one another.

This framework has three key elements: (1) affirmation that existing international law applies to state behavior in cyberspace; (2) development of an international consensus on and promotion of additional voluntary norms of responsible state behavior in cyberspace that apply during peacetime; and (3) development and implementation of practical confidence-building measures (CBMs) among states.

Since 2009, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) has served as a productive and groundbreaking expert-level venue for the United States to build support for this framework through three consensus reports in 2010, 2013, and 2015.

The conclusions captured in these reports have been endorsed by political leaders in a range of settings, including during the G20 summit in Antalya, Turkey, in 2015, and reaffirmed at the 2016 G20 summit in Hangzhou, China. Perhaps the most prominent bilateral statement of support for this framework came during Chinese President Xi Jinping's state visit to Washington in September 2015, when both the United States and China committed, *inter alia*, that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."

### Capacity Building

The United States can more effectively respond to foreign cyber threats and transnational crime when our international partners themselves have strong incident response and cybercrime fighting capabilities. Therefore, the Department of State is working with departments and agencies, allies, and multilateral partners to build the capacity of foreign governments, particularly in developing countries, to secure their own networks as well as to investigate and prosecute cybercriminals within their borders. The Department also actively promotes donor cooperation, including bilateral and multilateral participation in joint cyber capacity building initiatives.

In 2015, for example, the United States joined the Netherlands in founding the Global Forum on Cyber Expertise, a global platform for countries, international organizations, and the private sector to exchange best practices and expertise on cyber capacity building. The United States partnered with Japan, Australia, Canada, the African Union Commission, and Symantec on four cybersecurity and cybercrime capacity building initiatives. The Department also provided assistance to the Council of Europe, the Organization of American States, and the United Nations Global Program on Cybercrime, among others, to enable delivery of capacity building assistance to developing nations. Many traditional bilateral law enforcement training programs, including those focused on counterterrorism, increasingly include cyber elements, such as training investigators and prosecutors in the handling of electronic evidence. Much of our foreign law enforcement training on combatting intellectual property crime focuses on digital theft.

### Responding to Cyber Incidents

Over the past two years, we have witnessed a number of high-profile cyberattacks – at home and abroad – on financial institutions, private companies, government agencies, critical infrastructure, and political organizations.

The United States uses a whole-of-government approach to respond to and deter malicious activities in cyberspace that brings to bear its full range of instruments of national power and corresponding policy tools – diplomatic, law enforcement, economic, military, and intelligence – as appropriate and consistent with applicable law.

The State Department plays a key role in interagency deliberations on major cyber events, and it engages through diplomatic channels when needed. For example, during the 2012-2013 distributed denial-of-service (DDoS) attacks against financial institutions, diplomatic channels were used as a supplement to incident response efforts through more technical channels, ensuring that policy makers in foreign governments were aware of U.S. requests for assistance. We also have used diplomatic channels to raise concerns regarding the cyber-enabled theft of trade secrets for commercial gain.

### Combatting Transnational Crime

The United States is a global leader in the campaign against transnational crime. In partnership with key allies and multilateral partners, the U.S. helps countries effectively utilize existing legal tools, fund development of modern legal frameworks, provide training on cybercrime investigations, and strengthen international cooperation to combat modern, high-tech crime threats.

The State Department, with its interagency partners, actively promotes membership in the Council of Europe Convention on Cybercrime, known as the Budapest Convention, supports the Group of Seven (G7) 24/7 Network, and offers rewards for information leading to the arrest or conviction of members of transnational cybercrime organizations.

### Recommendations

As we look ahead, cybersecurity will continue to be a challenge for the United States when we take into consideration the rapidly expanding environment of global cyber threats, the increasing reliance on information technology, the reality that many developing nations are still in the early stages of their cyber maturity, and the ongoing and increasingly sophisticated use of information technology by terrorists and other criminals.

Therefore, we offer the following recommendations for the Commission’s consideration.

- Efforts to further strengthen the strategic framework of international cyber stability should continue through promotion of certain voluntary norms of responsible state behavior in cyberspace that apply during peacetime; expansion of global affirmation that international law applies to state behavior in cyberspace; and development and implementation of additional confidence building measures to reduce risks of misperception and escalation.

- The United States pursues a vision of openness and collaborative, multi-stakeholder governance for cyberspace, in stark contrast to alternative, state-centric concepts of cyberspace governance pursued by some countries, principally China and Russia. Therefore, the United States should continue to advocate in bilateral and multilateral fora, including the United Nations, toward multi-stakeholder governance for cyberspace.
- The ability of the United States to respond to foreign cyber threats and promote international cyber stability is greatly enhanced by the capabilities and strength of our international partners in this area. It is essential, therefore, to continue to build the capacity of foreign governments, particularly in developing countries, to secure their own networks, and to promote donor cooperation in joint capacity building initiatives.
- Given the transnational nature of the Internet and related communications infrastructure, international cooperation is essential to effectively address cyber incidents. This is especially true for the most serious cyber incidents of strategic concern that require an immediate response and those with significant cross-border implications. Therefore, the United States should continue efforts to enhance its understanding of other countries' cyber incident response and coordination capabilities and to formalize communications channels, including network defense, law enforcement, diplomatic, military, and others.
- To further combat transnational cybercrime, the United States should continue to expand its partnerships with allies and multilateral partners, promote membership in the Budapest Convention, enlarge the G7 24/7 Network, and target transnational cybercrime organizations.
- Here at home, the State Department should continue to mainstream cyberspace issues into our foreign diplomatic engagements and build the necessary internal capacity to formulate, coordinate, and implement cyber policy and execute our cyber diplomacy.

Lastly, to provide additional background information for the Commission's consideration on the State Department's work in this area, I am including with this statement two documents we submitted to Congress earlier this year – my Senate oversight testimony and the *Department of State International Cyberspace Policy Strategy*.

In closing, I would like to thank the Commission for giving me this opportunity to speak today, and I look forward to answering any questions you may have.

Note: Mr. Painter also provided links to the following external documents:

- Testimony before the Senate Foreign Relations Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, Hearing on "International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms," May 25, 2016. http://www.foreign.senate.gov/imo/media/doc/052516_Painter_Testimony.pdf
- Public Law 114-113, Division N, Title IV, Section 402, "Department of State International Cyberspace Policy Strategy," March 2016. http://www.state.gov/documents/organization/255732.pdf

## *Mark Ryland*

Good afternoon, Chairman Donilon, Vice-Chair Palmisano, and esteemed members of the Commission, my name is Mark Ryland. I serve as the senior technologist for the worldwide public sector for Amazon Web Services (AWS), a wholly owned subsidiary of Amazon.com. On behalf of AWS, thank you for giving me the opportunity to speak at this Commission session on how to embrace IT innovation in the government in order to enhance cybersecurity, which is what I was asked to speak about today.

### AWS and the Utility-based Model of Cloud

Just over 10 years ago, AWS began offering access to cloud-based infrastructure services based on Amazon's expertise in highly scaled infrastructure and service-oriented software. A decade later, a vast range of organizations from the smallest start-ups to the largest enterprises and government agencies have taken advantage of this flexible, secure, powerful, and highly efficient way of accessing IT resources.

Before the cloud, businesses and government agencies spent a lot of time and money managing their own datacenters and co-location facilities, which meant time not spent on their core organizational missions of providing products and services to their customers and citizens. With cloud, organizations like government agencies can function more like startups that move at the speed of ideas, without upfront costs or worry about unknown future capacity needs. Previously, organizations only had an option of either making massive capital investments to build their own data center and server infrastructure, or of entering into long-term contracts with a vendor for a fixed amount of data center capacity that they might or might not use. This choice meant either paying for wasted capacity sitting idle while waiting for rare occasions of peak demand, or worrying about shortages, i.e., that the capacity deployed was insufficient to meet peak demands.

Today, AWS has more than a million active customers in 190 countries, including more than 2,300 government agencies, 7,000 education institutions and 22,000 nonprofit organizations. AWS customers range from some of the world's most successful startups like Pinterest and Airbnb, to large enterprises in every kind of industry: companies such as Shell, BP, Johnson & Johnson, Pfizer, Merck, Bristol-Meyer Squibb, Capital One Bank, GE, Schneider Electric, Netflix, Samsung, Adobe, Time, News Corp, the Washington Post and the New York Times. In the public sector, our customers include federal, state, and local government organizations such as NASA, the U.S Securities and Exchange Commission, U.S. Department of Homeland Security, the State of Texas, the U.S. Department of Health & Human Services, the State of Arizona, New York City Department of Transportation, the City of Los Angeles (CA), King County (WA), and the Financial Industry Regulatory Authority (FINRA). In addition, thousands of educational institutions from Harvard, MIT, UC Berkeley, and Stanford to small school districts like one in Fish Creek, Wisconsin all utilize AWS for web-based IT services.

### Modernizing Government Technology/Security Benefits of Cloud Computing

In the beginning, there was a certain degree of reluctance to trust the large-scale, utility-style, multi-tenanted, so-called "public" cloud. This was understandable considering that any time a powerful new abstraction appears in the IT industry, it takes time for users to understand and become comfortable with it. Fifty years ago compilers were new and raised questions; just 10 years ago it was virtualization. More recently, it was cloud.

But as customers and IT professionals have learned about the cloud and its capabilities, the initial concerns have turned around completely. Now there is a growing realization that commercial cloud service providers offer fundamental security benefits over traditional IT infrastructure. As U.S. Federal CIO Tony Scott has stated, "I see the big cloud providers in the same way I see a bank. They have the incentive, they have skills and abilities, and they have the motivation to do a much better job of security than any one company or any one organization can probably do. [...] I think today the better bet is get to the cloud as quick as you can because you're guaranteed almost to have better security there than you will in any private thing you can do."[7]

The following are "Seven Reasons for the Systemic Superiority of Cloud Security" that I would like to emphasize for today's session:

(1) the integration of compliance (which you can think of as security policy) and actual, operational security (something seldom accomplished in traditional systems);

(2) economies of scale apply to security personnel and processes, something large scale cloud service providers are uniquely able to deliver;

(3) with the cloud provider taking on a major portion of the security "surface area," and executing that with professional focus and skill beyond almost any customer on earth, customers can refocus their security professionals and resources on a much smaller part of the challenge (specifically, application security);

(4) the cloud provides visibility, homogeneity, and automation never seen before in traditional systems, all of which massively benefit security;

(5) commercial cloud services are "systems containers" that surround traditional systems and provide far more insight into their behavior and functioning, including security issues, thereby providing a new kind of "defense in depth";

(6) with easy and cheap access to massive amounts of storage and processing capacity, our customers use the cloud to secure the cloud, i.e., they run big data analytics on security data and log data which provides far more insight into their security posture and results in a much faster remediation of issues; and

(7) finally, with the speed of innovation and increasing scale, the cloud security story will only get better, and do so quickly!

In short, the commercial cloud and its accompanying automation and agility provide a unique opportunity to *enhance* systems security and privacy. As a former senior government security official said, when asked about the growing cybersecurity threats to government networks at a recent closed-door cybersecurity event at the American Enterprise Institute, "Cloud gives us a 'mulligan'; a chance to do it over and do it right." In sum, we believe the evidence fully supports the proposition that security should no longer be seen as a *barrier* to cloud adoption, but an argument in *favor* of it.

That is why the U.S. the intelligence community has turned to the cloud to serve customers across the 17 intelligence agencies,[8] that is why commercial companies with sensitive information ranging from financial institutions to healthcare providers are leveraging cloud to meet their digital infrastructure needs, and that is why government agencies such as the Federal Aviation Administration (FAA), the Department of Health and Human Services (HHS), the State of Colorado, the Seattle Police Department, the State of Minnesota, the California Department of Justice (DoJ), and the U.S. Department of Homeland Security (DHS) are also moving mission-critical and sensitive workloads that serve and protect Americans to the commercial cloud.

Here are what some of our most security-conscious customers have said about security in the AWS cloud:

"*From a physical and logical security standpoint, I believe that, if done right, public cloud computing is as or more secure than self-hosting*." – Steve Randich, EVP and CIO, Financial Industry Regulatory Authority in the USA

[7] http://www.cio.com/article/2996268/cloud-computing/us-cio-tells-it-leaders-to-trust-the-cloud.html

[8] http://www.govexec.com/magazine/features/2014/07/daring-deal/88207/

"*And of course, security is critical for us. The financial services industry attracts some of the worst cyber criminals. So we worked closely with the AWS team to develop a security model which, we believe, allows us to operate more securely in the public cloud than we can even in our own datacenters*." Rob Alexander, CIO, Capital One Bank

"*Based on our experience, I believe that we can be even more secure in the AWS cloud than in our own datacenters*." -Tom Soderstrom, CTO, NASA's Jet Propulsion Lab

**Recommendations**

We applaud the Administration's emphasis on cybersecurity with a specific focus on securing federal networks and planning for building security into emerging technologies such as IoT. The Administration's "Cloud First" policy should continue to serve as the foundation of improving the federal government cybersecurity posture. But we believe there is more to be done.

To fully realize the goals of the President's Cybersecurity National Action Plan ("CNAP"), AWS recommends the following: First, the Commission should recognize that the most important step forward in the effort to secure government communications networks and IT systems per the CNAP is through effective and lasting technology modernization. As noted just a few days ago by Federal CIO Tony Scott, the government must stop using a "bubble wrap" approach, putting fragile security layers around inherently insecure legacy systems.[9] In the private sector, IT modernization is happening because businesses of all sizes, and across all sectors of the economy, are moving their applications and workloads into the commercial cloud. Yet policy, regulatory, procurement, and cultural blockers still remain that prevent federal departments and agencies from migrating to cloud. We think the Commission should call on the OMB to fully enforce the "Cloud First" policy, and closely scrutinize current and future government data center utilization.

Second, the Commission should call on both the Administration and Congress to fully enforce the Federal Information Technology Acquisition Reform Act (FITARA) to ensure that agency chief information officers have the procurement resources to modernize IT systems as quickly as possible. Additionally, the Commission should support the passage of the recently introduced Modernizing Government Technology (MGT) Act, which was approved by the House Oversight and Government Reform Committee last week. The MGT Act provides a mandate for IT modernization through commercial cloud adoption and the replacement/retirement of outdated legacy systems that are vulnerable to cyber-attacks. This important legislation could also provide the necessary funding flexibility for agencies to more quickly leverage a secure IT infrastructure such as commercial cloud computing services.

Third, given the importance of FedRAMP to ensuring a baseline of security for government organizations, we recommend that Congress require that cloud service providers (CSPs) or contractors delivering cloud services to federal agencies complete a security assessment under FedRAMP. That will give federal agencies clarity on what security baseline CSPs and contractors should be compliant with.

Finally, just as FedRAMP has provided a security baseline for the federal government, the Commission should encourage state and local governments to leverage the FedRAMP requirements and processes as their primary security certification framework for IT systems. Doing so will help state and local government agencies to build a secure IT ecosystem.

Thank you for holding this meeting today and inviting us to participate. I look forward to discussing these critical issues with you and the other panelists.

[9] http://fedscoop.com/tony-scott-cybersecurity-billington-september-2016

## *Mike Walker*

Large breaches of confidential records are a regular occurrence on today's internet. This is not due to structural failures of the Internet protocols themselves, nor is it due to poor user choices, nor even to insufficient demand for effective security. The vast majority of breaches occur due to a structural failure of software, often software that handles email links or attachments, but many other forms of software as well. Structural failures of software are common amongst all market sectors where we currently experience a lack of trust & confidence: SCADA, the desktop, vehicles, life safety medical appliances and critical infrastructure. In order to rebuild cyber trust in these sectors, we must create a way to engineer software systems in a trustworthy manner, measure residual cyber risk, and accurately price insurance of these software systems; this requires:

1> an ability to create and manage systems that are engineered to be stronger by design

2> the ability to measure the vulnerability of software systems

These two thrusts are complimentary: more secure systems can only be developed or selected when the market can easily appraise the security of software systems; without measurement it is impossible for a market to find and fund a more secure approach. Universally accepted measurement of vulnerability is therefore a prerequisite for security standards that can survive operational scrutiny. Measurement of vulnerability occurs through exhaustive investigation rather than the satisfaction of checklists. Exhaustive investigation is an expert task currently procured through bug bounties. Revolutionary automated approaches on the horizon may soon democratize such exhaustive investigation and allow for a universal, independently testable standard for software safety.

## *Gregory C. Wilshusen*

Chairman Donilon, Vice Chair Palmisano, and distinguished members of the Commission, thank you for the opportunity to appear before you today. As requested, I will discuss laws and policies shaping the federal government's information technology (IT) security landscape and the actions needed to address long-standing challenges to improving the government's cybersecurity posture.

My name is Greg Wilshusen and I serve as the Director of Information Security Issues for the U.S. Government Accountability Office (GAO). GAO is an independent agency in the legislative branch of the federal government. Our mission is to help Congress improve the performance and accountability of the federal government for the benefit of the American people. In other words, we examine how taxpayer dollars are spent and advise lawmakers and agency heads on ways to make government work better. In my position, I am responsible for leading audits and studies of the security of federal information systems and cyber critical infrastructure and the privacy of personally identifiable information. My statement today is based on our previously published work addressing federal cybersecurity efforts.[10]

As computer technology has advanced, federal agencies have become dependent on computerized information systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. Virtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, ineffective controls can result in significant risk to a broad array of government operations and assets. For example:

- Resources, such as payments and collections, could be lost or stolen.
- Computer resources could be used for unauthorized purposes, including launching attacks on others.
- Sensitive information, such as intellectual property and national security data, and personally identifiable information, such as taxpayer data, Social Security records, and medical records, could be inappropriately added to, deleted, read, copied, disclosed, or modified for purposes such as espionage, identity theft, or other types of crime.
- Critical operations, such as those supporting national defense and emergency services, could be disrupted.
- Data could be modified or destroyed for purposes of fraud or disruption.
- Entity missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and fulfill their responsibilities.

Federal information systems and networks are inherently at risk. They are highly complex and dynamic, technologically diverse, and often geographically dispersed. This complexity increases the difficulty in identifying, managing, and protecting the myriad of operating systems, applications, and devices comprising the systems and networks. Compounding the risk, systems used by federal agencies are often riddled with security vulnerabilities—both known and unknown. For example, the national vulnerability database maintained by the Mitre Corporation has identified 78,907 publicly

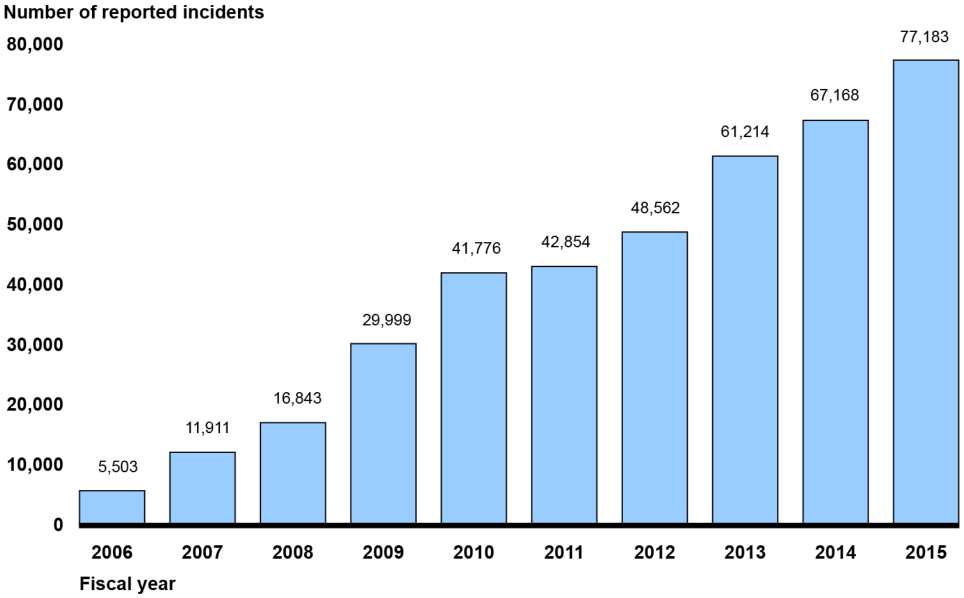
[10] The reports cited in this statement contain detailed discussions of the scope of the work and the methodology used to carry it out. All the work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

known cybersecurity vulnerabilities and exposures as of September 15, 2016, with more being added each day.[11] Federal systems and networks are also often interconnected with other internal and external systems and networks including the Internet, thereby increasing the number of avenues of attack and expanding their attack surface.

In addition, cyber threats and incidents to systems supporting the federal government are increasing. These threats come from a variety of sources and vary in terms of the types and capabilities of the actors, their willingness to act, and their motives. For example, advanced persistent threats—where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risks. Further underscoring this risk are increases in incidents that could threaten national security and public health and safety, or lead to inappropriate access to and disclosure, modification, or destruction of sensitive information. Such incidents may be unintentional, such as a service disruption due to equipment failure or natural event, or intentional, where for example, a hacker attacks a computer network or system.

The number of information security incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (U.S. CERT) has continued to increase—from 5,503 in fiscal year 2006 to 77,183 in fiscal year 2015, an increase of 1,303 percent (see fig. 1 below).

**Figure 1: Incidents Reported by Federal Agencies, Fiscal Years 2006 through 2015**



Source: GAO analysis of United States Computer Emergency Readiness Team and Office of Management and Budget data for fiscal years 2006-2015. | GAO-16-885T

Since 1997, we have designated federal information security as a government-wide high-risk area,[12] and in 2003 expanded this area to include computerized systems supporting the nation's critical infrastructure. Most recently, in the February 2015 update to our high-risk list, we further expanded

[11] The national vulnerability database is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance.

[12] GAO designates agencies and program areas as high-risk due to their vulnerabilities to fraud, waste, abuse, and mismanagement, or when they are most in need of transformation.

this area to include protecting the privacy of personally identifiable information (PII) collected, maintained, and shared by both federal and nonfederal entities.[13]

Over the last several years, we have made about 2,500 recommendations to agencies aimed at improving their implementation of information security controls. These recommendations identify actions for agencies to take in protecting their information and systems. For example, we have made recommendations for agencies to correct weaknesses in controls intended to prevent, limit, and detect unauthorized access to computer resources, such as controls for protecting system boundaries, identifying and authenticating users, authorizing users to access systems, encrypting sensitive data, and auditing and monitoring activity on their systems. We have also made recommendations for agencies to implement their information security programs and protect the privacy of PII held on their systems. However, many agencies continue to have weaknesses in implementing these controls, in part because many of these recommendations remain unimplemented. As of September 16, 2016, about 1,000 of our information security–related recommendations have not been implemented.

**Federal Law and Policy Establish a Framework for Protecting Federal Systems and Information**

Several federal laws and policies—predominantly the Federal Information Security Modernization Act of 2014 and its predecessor, the Federal Information Security Management Act of 2002 (both referred to as FISMA)—provide a framework for protecting federal information and IT assets.

The purpose of both laws is to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.[14] The laws establish responsibilities for implementing the framework and assign those responsibilities to specific officials and agencies:

- The Director of the Office of Management and Budget (OMB) is responsible for developing and overseeing implementation of policies, principles, standards, and guidelines on information security in federal agencies, except with regard for national security systems. Since 2003, OMB has issued policies and guidance to agencies on many information security issues, including providing annual instructions to agencies and inspectors general for reporting on the effectiveness of agency security programs. More recently, OMB issued the *Cybersecurity Strategy and Implementation Plan* in October 2015,[15] which aims to strengthen federal civilian cybersecurity by (1) identifying and protecting high-value information and assets, (2) detecting and responding to cyber incidents in a timely manner, (3) recovering rapidly from incidents when they occur and accelerating the adoption of lessons learned from the sprint, (4) recruiting and retaining a highly qualified cybersecurity workforce, and (5) efficiently acquiring and deploying existing and emerging technology. OMB also recently updated its Circular A-130 on managing federal information resources to address protecting and managing federal information resources and on managing PII.[16]
- The head of each federal agency has overall responsibility for providing appropriate information security protections for the agency's information and information systems, including those collected, maintained, operated or used by others on the agency's behalf. In addition, the head of each agency is required to ensure that senior agency officials provide

[13] See GAO, *High-Risk List: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

[14] The Federal Information Security Modernization Act of 2014 (FISMA 2014) (Pub. L. No. 113-283, Dec. 18, 2014); largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as title III of the E-Government Act of 2002 (Pub. L. No. 107-347, 116 Stat 2899, 2946 (Dec. 17, 2002)). As used here, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect

[15] OMB, *Cybersecurity Strategy and Implementation Plan for Federal Civilian Government*, M-16-04 (Washington, D.C.: Oct. 30, 2015).

[16] OMB, Revision of OMB Circular A-130, *Managing Federal Information as a Strategic Resource* (Washington, D.C.: July 28, 2016).

information security for the information and systems supporting the operations and assets under their control, and the agency chief information officer (CIO) is delegated the authority to ensure compliance with the law's requirements. The assignment of information security responsibilities to senior agency officials is noteworthy because it reinforces the concept that information security is a business function as well as an IT function.

Each agency is also required to develop, document, and implement an agency-wide information security program that involves an ongoing cycle of activity including (1) assessing risks, (2) developing and implementing risk-based policies and procedures for cost-effectively reducing information security risk to an acceptable level, (3) providing awareness training to personnel and specialized training to those with significant security responsibilities, (4) testing and evaluating effectiveness of security controls, (5) remedying known weaknesses, and (6) detecting, reporting, and responding to security incidents.

As discussed later, our work has shown that agencies have not fully or effectively implemented these programs and activities on a consistent basis.

- FISMA requires the National Institute of Standards and Technology (NIST) to develop information security standards and guidelines for agencies. To this end, NIST has developed and published federal information processing standards that require agencies to categorize their information and information systems according to the impact or magnitude of harm that could result if they are compromised[17] and specify minimum security requirements for federal information and information systems.[18] NIST has also issued numerous special publications that provide detailed guidelines to agencies for securing their information and information systems.[19]
- In 2014, FISMA established the Department of Homeland Security's (DHS) oversight responsibilities, including (1) assisting OMB with oversight and monitoring of agencies' information security programs, (2) operating the federal information security incident center, and (3) providing agencies with operational and technical assistance.

Other cybersecurity-related laws were recently enacted, which include the following:

- The National Cybersecurity Protection Act of 2014 codifies the role of DHS's National Cybersecurity and Communications Integration Center as the federal civilian interface for sharing information about cybersecurity risks, incidents, analysis, and warnings for federal and non-federal entities, including owners and operators of systems supporting critical infrastructure.[20]
- The Cybersecurity Enhancement Act of 2014, among other things, authorizes NIST to facilitate and support the development of voluntary standards to reduce cyber risks to critical infrastructure and, in coordination with OMB, to develop and encourage a strategy for the adoption of cloud computing services by the federal government.[21]

[17] NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: February 2004).

[18] NIST, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS Publication 200 (Gaithersburg, Md.: March 2006).

[19] For example, NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, Rev. 1 (Gaithersburg, Md.: February 2010) and *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Rev. 4 (Gaithersburg, Md.: April 2013).

[20] Pub. L. No. 113-282, Dec. 18, 2014.

[21] Pub. L. No. 113-274, Dec. 18, 2014.

- The Cybersecurity Act of 2015, among other things, sets forth authority for enhancing the sharing of cybersecurity-related information among federal and non-federal entities, gives DHS's National Cybersecurity and Communications Integration Center responsibility for implementing these mechanisms, requires DHS to make intrusion and detection capabilities available to any federal agency, and calls for agencies to assess their cyber-related workforce.[22]

## Action Is Needed to Address Ongoing Cybersecurity Challenges

Our work has identified the need for improvements in the federal government's approach to cybersecurity. While the administration and agencies have acted to improve the protections over their information and information systems, additional actions are needed.

**Federal agencies need to effectively implement risk-based entity- wide information security programs consistently over time.** Since FISMA was enacted in 2002, agencies have been challenged to fully and effectively develop, document, and implement agency-wide programs to secure the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency or contractor. For example, in fiscal year 2015, 19 of the 24 major federal agencies covered by the Chief Financial Officers Act of 1990[23] reported that information security control deficiencies were either a material weakness or significant deficiency[24] in internal controls over financial reporting. In addition, inspectors general at 22 of the 24 agencies cited information security as a major management challenge for their agency. The following actions will assist agencies in implementing their information security programs.

- *Enhance capabilities to effectively identify cyber threats to agency systems and information.* A key activity for assessing cybersecurity risk and selecting appropriate mitigating controls is the identification of cyber threats to computer networks, systems, and information. In 2016, we reported on several factors that agencies identified as impairing their ability to identify these threats to a great or moderate extent.[25] The impairments included an inability to recruit and retain personnel with the appropriate skills, rapidly changing threats, continuous changes in technology, and a lack of government-wide information-sharing mechanisms. Addressing these impairments will enhance the ability of agencies to identify the threats to their systems and information and be in a better position to select and implement appropriate countermeasures.
- *Implement sustainable processes for securely configuring operating systems, applications, workstations, servers, and network devices*. We routinely determine that agencies do not enable key information security capabilities of their operating systems, applications, workstations,

[22] The Cybersecurity Act of 2015 was enacted as Division N of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Dec. 18, 2015.

[23] The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development. 31 U.S.C. § 901(b).

[24] A material weakness is a deficiency, or combination of deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis.

[25] GAO, *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.; May 18, 2016).

servers, and network devices. In many instances, agencies were not aware of the insecure settings that introduced risk to the computing environment. Establishing strong configuration standards and implementing sustainable processes for monitoring and enabling configuration settings will strengthen the security posture of federal agencies.

- *Patch vulnerable systems and replace unsupported software*. Federal agencies consistently fail to apply critical security patches in a timely manner on their systems, sometimes years after the patch is available. We also consistently identify instances where agencies use software that is no longer supported by their vendors. These shortcomings often place agency systems and information at significant risk of compromise since many successful cyberattacks exploit known vulnerabilities associated with software products. Using vendor-supported and patched software will help to reduce this risk.
- *Develop comprehensive security test and evaluation procedures and conduct examinations on a regular and recurring basis.* The information security assessments performed for agency systems were often based on interviews and document reviews, limited in scope, and did not identify many of the security vulnerabilities that our examinations identified. Conducting in-depth security evaluations that examine the effectiveness of security processes and technical controls is essential for effectively identifying system vulnerabilities that place agency systems and information at risk.
- *Strengthen oversight of contractors providing IT services.* As demonstrated by the OPM data breach of 2015, cyber attackers can sometimes gain entrée to agency systems and information through the agency's contractors or business partners. Accordingly, agencies need to ensure that their contractors and partners are adequately protecting the agency's information and systems. In August 2014, we reported that five of six selected agencies were inconsistent in overseeing the execution and review of security assessments that were intended to determine the effectiveness of contractor implementation of security controls, resulting in security lapses.[26] In 2016, agency chief information security officers we surveyed reported that they were challenged to a large or moderate extent in overseeing their IT contractors and receiving security data from the contractors, thereby diminishing the CISOs' ability to assess how well agency information maintained by the contractors is protected.[27] Effectively overseeing and reviewing the security controls implemented by contractors and other parties is essential to ensuring that the organization's information is properly safeguarded.

**The federal government needs to improve its cyber incident detection, response, and mitigation capabilities.** Even agencies or organizations with strong security can fall victim to information security incidents due to previously unknown vulnerabilities that are exploited by attackers to intrude into an agency's information systems. Accordingly, agencies need to have effective mechanisms for detecting, responding to, and recovering from such incidents. The following actions will assist the federal government in building its capabilities for detecting, responding to, and recovering from security incidents.

- *DHS needs to expand capabilities, improve planning, and support wider adoption of its government-wide intrusion detection and prevention system.* In January 2016, we reported that DHS's National Cybersecurity Protection System (NCPS) had limited capabilities for detecting and preventing intrusions, conducting analytics, and sharing information.[28] In addition, adoption of these capabilities at federal agencies was limited. Expanding NCPS's capabilities

[26] GAO, *Information Security: Agencies Need to Improve Oversight of Contractor Controls*, GAO-14-612 (Washington, D.C.: Aug. 8, 2014).

[27] GAO, *Federal Chief Information Security Officer: Opportunities Exist to Improve Roles and Address Challenges to Authority*, GAO-16-686 (Washington, D.C.: Aug. 26, 2016).

[28] GAO, *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, GAO-16-294 (Washington, D.C.: Jan. 28, 2016).

for detecting and preventing malicious traffic, defining requirements for future capabilities, and developing network routing guidance would increase assurance of the system's effectiveness in detecting and preventing computer intrusions and support wider adoption by agencies.

- *Improve cyber incident response practices at federal agencies*. In April 2014 we reported that 24 major federal agencies did not consistently demonstrate that they had effectively responded to cyber incidents.[29] For example, agencies did not determine the impact of incidents or taken actions to prevent their recurrence. By developing complete policies, plans, and procedures for responding to incidents and effectively overseeing response activities, agencies will have increased assurance that they will effectively respond to cyber incidents.
- *Update federal guidance on reporting data breaches and develop consistent responses to breaches of personally identifiable information (PII).* As we reported in December 2013, eight selected agencies did not consistently implement policies and procedures for responding to breaches of PII.[30] For example, none of the agencies documented the evaluation of incidents and lessons learned. In addition, OMB's guidance to agencies to report each PII-related incident—even those with inherently low risk to the individuals affected—within 1 hour of discovery may cause agencies to expend resources to meet reporting requirements that provide little value and divert time and attention from responding to breaches. Updating guidance and consistently implementing breach response practices will improve the effectiveness of government-wide and agency-level data breach response programs.

**The federal government needs to expand its cyber workforce planning and training efforts.** Ensuring that the government has a sufficient number of cybersecurity professionals with the right skills and that its overall workforce is aware of information security responsibilities remains an ongoing challenge. These actions can help meet this challenge:

- *Enhance efforts for recruiting and retaining a qualified cybersecurity workforce.* This has been a long-standing dilemma for the federal government. In 2012, agency chief information officers and experts we surveyed cited weaknesses in education, awareness, and workforce planning as a root cause in hindering improvements in the nation's cybersecurity posture.[31] Several experts also noted that the cybersecurity workforce was inadequate, both in numbers and training. They cited challenges such as the lack of role-based qualification standards and difficulties in retaining cyber professionals. In 2016, agency CISOs we surveyed reported that difficulties related to having sufficient staff; recruiting, hiring, and retaining security personnel; and ensuring security personnel have appropriate skills and expertise pose challenges to their abilities to carry out their responsibilities effectively.[32]
- *Improve cybersecurity workforce planning activities at federal agencies.* In November 2011, we reported that only five of eight selected agencies had developed workforce plans that addressed cybersecurity.[33] Further, agencies reported challenges with filling cybersecurity positions, and only three of the eight had a department- wide training program for their cybersecurity workforce.

[29] GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices*, GAO-14-354 (Washington, D.C.: Apr. 30, 2014).

[30] GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, GAO-14-34 (Washington, D.C.: Dec. 9, 2013).

[31] GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187 (Washington, D.C.: Feb. 14, 2013).

[32] GAO-16-686.

[33] GAO, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination*, GAO-12-8 (Washington, D.C.: Nov. 29, 2011).

In summary, federal law and policy set forth a framework for addressing cybersecurity risks to federal systems. However, implementation of this framework has been inconsistent, and additional action is needed to address ongoing challenges. Specifically, agencies need to address control deficiencies and fully implement organization-wide information security programs, cyber incident response and mitigation efforts need to be improved across the government, and establishing and maintaining a qualified cybersecurity workforce needs to be a priority.

Chairman Donilon, Vice Chair Palmisano, and distinguished members of the Commission, this concludes my prepared statement. I would be happy to answer any questions you have.

## Contact and Acknowledgments

If you have any questions about this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other staff members who contributed to this statement include Larry Crosland and Michael Gilmore (assistant directors), Chris Businsky, Franklin Jackson, Kenneth A. Johnson, Lee McCracken, Scott Pettis, and Adam Vodraska.

## *Neal Ziring*

Chairman Donilon, Vice-Chairman Palmison, and distinguished members of the commission, thank you for this opportunity to participate today, and provide input on this very important topic. My name is Neal Ziring, and I serve as the Technical Director for Capabilities at the National Security Agency. Prior to that job, I served five years as Technical Director for Information Assurance at NSA.

NSA has the responsibility, under National Security Directive 42, to protect and defend U.S. National Security Systems (NSS). I've worked in that mission at NSA for 28 years. NSA defends our country's most sensitive information and networks from motivated and persistent adversaries, and assists other elements of the U.S. federal government with technical challenges spanning all aspects of cybersecurity. I've enjoyed a front-row seat for a great deal of that, and the observations and recommendations I'll offer this afternoon are founded on those experiences, and on discussions with my peers in NSA and across the community.

I must note that my remarks today do not represent NSA's official position, but are merely my own views as a technical practitioner and leader.

The topic for this panel is "growing and securing the digital economy". This will be vital for the future of our country and world, as the digital economy is woven throughout the entire economy. Unlike the early 1990s, where activity on the nascent Internet was largely independent of the rest of the social and economic activity, today, we depend on our networks for everything including critical infrastructure, finances, and national defense. Growing and enriching the digital economy can only be achieved by sustaining and building up all stakeholders' confidence in the underpinnings of that economy, i.e., confidence in cyberspace.

There are a lot of key stakeholders to consider: businesses, consumers, service providers, government agencies, investors, law enforcement, critical infrastructure operators, and more. As part of my work for NSA, I've participated in partnerships across government, industry, academia and international allies. Based on my interactions with these various partners, it is clear that we're all working toward the same confidence in cyberspace goal. The common purpose is also evident in the statements offered by participants in previous open meetings of this Commission.

In my remarks today, I'll cover a few aspects of the current situation that I think are most critical, and then offer some general recommendations for action that we could take as a nation, both short-term and long-term. Then, of course, I'll be happy to address any questions the Commission may pose.

### **Some Aspects of the Current State of Cybersecurity**

Previous panelists for this commission have covered current threats and risks quite thoroughly; to save time, I'm going to review just a few items that will help lead into my recommendations.
First and most critical: we all share the same cyberspace. The trend of convergence over the last couple of decades has brought nearly all networks together. Even networks that are ostensibly "stand alone" have some connection or direct dependence on the global Internet. This directly affects the reliability and security of services we all depend on, including critical infrastructures. Just to cite one example: consider the global Signaling System 7 (SS7) network. Network operators connect to it with systems that are also connected to the Internet; SS7 traffic crosses the same fibers as other traffic, and at the endpoints, SMS messages that cross the SS7 network can cause smartphones to take Internet actions. There are many more examples. The point I'd like to make is that isolated islands are rarely actually isolated, but many of them are secured and defended as if they were.

Next, malicious actors and criminals follow value. As the U.S. and other countries have shifted more of our economic, governmental, and social activities into cyberspace, the motivations increase for threat actors to shift their activities there too. We've seen endless examples of this. Value can be found in something as simple as money, or as abstract as geopolitical influence.

Third, today's security features, standards, and practices are better than they ever were. In most areas, they've progressed enormously since I entered this field in the late 1980s. That should make exploitation of connected systems harder. Several factors have preserved the exploitability of systems, even as the components that comprise them have gotten more secure. Some important factors are as follows.

- Security is not consistent. Some portion of the individual components that make up our systems are insecure, badly configured, or out of date. Therefore, most systems have points of vulnerability, and attackers have developed effective tradecraft to find them. It is not possible to eliminate all points of vulnerability, but currently, they are far too common. (Note also, while security has improved for many elements of cyberspace, the rapid growth of cyber-physical systems, aka "Internet of Things", seems to be recapitulating old mistakes).
- Trust relationships are everywhere. They criss-cross every part of cyberspace, offering attackers avenues for leveraging initial access into exploitation of value. Trust relationships are essential to the digital economy, but they are currently subject to inadequate control.
- Defense of cyberspace is largely executed on an individual basis, person by persons, enterprise by enterprise. This allows attackers to gain repeated benefit from each tradecraft or tool investment because each enterprise or community must independently learn to recognize and defeat it. this is an area where we've made significant progress in recent years, and detection of some tradecraft elements has become more of a shared endeavor, mediated by security companies, sector councils, and consortia. Better detection is useful but not sufficient.
- State-sponsored actors do not limit their activities to state targets, but instead, exploit any entity that might afford a path to their goals. This is a fundamentally asymmetric situation-state actors have resources and accesses that individual private sector companies cannot match. This asymmetry is fatal to the confidence necessary for growing the digital economy.
- Scale. As our networks have grown, and all sectors of our society have taken up cyberspace, the scale of this problem has exploded. And yet, a great deal of defense of these networks is still performed manually. This is costly or impossible to scale up, and it is too slow. (A basic goal of cyber defense is to respond to an intrusion or compromise before the attacker can gain value of it, manual operations cannot often accomplish this).
- Finally, we face a shortage of skilled and educated workers to take on roles securing and defending the digital economy. This shortage is reflected at every level, from basic entry-level network managers to senior researchers. The technologies of cyberspace will continue to grow and change, and attackers will continue to develop new tradecraft. Without a solid workforce, we will not be able to maintain or improve security in the long term.

## **Recommendations**

### *Hardening and Hygiene*

The hardest thing we need to do is to raise the basic level of security, both security functionality across products and services, and the security hygiene of connected systems. Components and systems can never be perfectly hardened against intrusions, but they can and must be better than what we have today.

Products and services must implement core security functionality, and users of those systems must have confidence that the functions were validated and are maintained. For most enterprise IT components, such as server operating systems, network devices, and office applications, suppliers are largely good at incorporating these functions. The next challenge is ensuring that they're enabled by default, and are maintained over a product's lifetime.

In other areas, even basic security functionality is not yet consistently available, and default configurations are often insecure. A few of the areas where this has been reported and independently confirmed industrial control systems, vehicle telemetric systems, and mobile applications. Certification programs can be effective at promoting industry improvement, such as the National Information Assurance Partnership (NIAP) for IT components, and the Federal Risk Assessment and Management Program (FedRAMP) for cloud services. But pressure from consumer and business customers is more effective, whether driven by regulation or incentive programs. Further, it is up to government and industry to collaborate to set the standards against which products and services should be certified- most recent NIAP Protection Profile requirements have been defined by technical committees with membership from government agencies, industry leaders, and often international partnerships. This approach has worked well and should be extended.

Enterprises must improve the consistency of security configuration and practice. This challenge is widely understood, and many enterprises have undertaken programs to improve their own cyber hygiene, just as the Department of Defense is doing right now. One critical factor for success is for an enterprise to really understand the risks they face, so they are motivated to actively manage them. The cybersecurity framework published by NIST in 2014 is one means of doing this, and has proven effective in many industry sectors. Driving wider adoption of the framework would boost cybersecurity across multiple parts of the digital economy.

Individual consumers, however, do not have the resources to undertake risk analyses and invest in securing their network services. Boosting security in this realm will require a coordinated strategy of awareness, product improvement, and incentives to keep systems maintained. There are several things we can do in the short term; here are two specific recommendations:

- **Credential Protection:** On-line service providers should offer basic fraud detection, notification, and response services for consumer accounts. Many of the larger providers already do this, but there are no standards or recognition for it. This is an area where government can and must work with industry to establish standards, and then promote adoption of those standards through consumer protection mechanisms.
- **Improved Domain Name Services:** The Domaine Name Service (DNS) is a foundational service for all consumer Internet users, and it is frequently abused by threat actors to support their malicious activities. These abuses are well-known and tracked by security companies and network service providers. All consumers should be provided DNS which protects them by default from known malicious sites and mappings (opt-out should always be offered too, but most consumers won't need it).

*Shared Defense*

Hardening will never be perfect, and even a highly secure system may be exposed through trust relationships. Therefore, we should always be prepared to defend systems during attacks, and recover them if attacks succeed. As I noted earlier, most defense today is conducted on an individual basis, thus permitting threat actors to leverage tradecraft investment across many targets. Information sharing is a part of this, and within certain industry sectors it is already providing great benefit. But we must work toward practices and technologies that will permit cooperative, integrated shared defense. There are three elements of shared defense that I'd like to describe today.

- First, broad information sharing is necessary, and at machine speeds. This will require both technical supports, such as data formats and transport services, and legal supports, such as clear authorities, rights and protections. Some solid technical standards already exist, such as the Security Content Automation Protocol (SCAP) specifications from NIST, and the Structured Threat Information eXpression (STIX) requirements from DHS. U.S. government agencies are leading the way on providing information in these formats, but there is far more we could do. Most importantly, government must set the example by being a full participant in cyber threat information sharing.

- Second, we need a robust, trusted, instrumented network infrastructure. This is an essential part of creating a defensible cyberspace. Network operators in the U.S. protect their own internal systems: the main exposure is at the seams between them. Security best practices exist for many core infrastructure services, such as Border Gateway Protocol (BGP) routing and SS7 messaging. These need to be comprehensively applied, ideally as a condition of offering carrier services in the U.S. market. The DNS infrastructure must also be trusted, and a mature DNS Security (DNSSec) standard exists. Government and industry will need to work together to make that DNSSec ubiquitous. Once this is done, there will be tremendous benefits to digital economy, because DNS will be able to serve as a base for other secure services.
- Third, we need to build mechanisms for automated, orchestrated and timely national response to cyberattacks. Today, the primary mechanism is for coordinating defensive responses among government and industry stakeholders is through holding video teleconferences and publishing advisories. Those who are not fast enough risk impacts from a catastrophic new vulnerability or large scale attack. This is a situation where government must take the lead, initially with network operators and then with a broader spectrum of cyberspace service providers. Together, stakeholders must work out a common response course of action, trigger mechanisms, and secure communication channels for coordinated action. it will take a lot of hard work, but luckily some of it is already in progress.

*Identity and Trust*

Trust relationships are built on identity and authentication, and they are essential to confidence in cyberspace. To enable the growth and diversification of the digital economy, we will need an array of services for identity, authentication, and associated services. The National Strategy for Trusted Identities in Cyberspace (NSTIC) was started in April 2011, with the intent of kick starting the development of such an identity and trust ecosystem. It has made some progress, but much more needs to be done.

An important aspect of the identity ecosystem must be the ability to securely associate attributes with identities. For example, I have an identity as a federal employee, embodied by a public key certificate and an associated private key stored on my DoD Common Access Card. This allows me, for example, to send a signed email that allows a recipient anywhere in the world to validate that the email came from me. (Individual consumers don't have this easily available to them, and that is one of the many challenges that the NSTIC set out to address). But I need to be able to do more than assert my identity, I need to be able to securely assert attributes, such as my employment status with the NSA, or that I'm authorized to work on a particular program, or that I have a certain insurance. Requirements for these kinds of assertions crop up throughout digital economy, but means for supporting them vary widely.

This is an area where the U.S. government can lead by example, by endorsing and then using relevant standards, and supporting capabilities for parties to make secure assertions, initially about employees, but perhaps eventually about any civilian.

Finally, any identity ecosystem must support rapid, trusted response to compromise of identity credentials. There are a few technical standards to help support this, but a few common practices or policies. This is an area where industry will probably have to lead, but government could help to bring stakeholders together and promote a common baseline.

*International Partnering*

The U.S. will realize the greatest benefit when we enhance our own cybersecurity in concert with other nations. There are many steps that the U.S. can take on its own, but most of those are more effective when they're global. In particular, the trust relationships that act as the topography of the digital economy often cross national boundaries.

First, information sharing and cyber situational awareness can and should be extended to U.S. allies, both government-to-government, and within various industry sectors. This has already begun in some areas, such as via traditional intelligence and law enforcement partnerships, but it needs to become the common practice. Cyber threat actors thrive on ignorance among their targets; by sharing information to create a common, multi-national view of cyberspace, we improve all participants defense.

Realizing this benefit will probably require several steps. We can begin with bi-lateral agreements to share threat indicators, malware samples, and network traffic statistics directly (machine-to-machine). Later steps could include pooling of data within existing treaties. Much of the relevant information is held by private sector entities such as network operators, but policy and legal barriers prevent them from pooling their knowledge. This may be a case where governments need to act as the hubs for shared visibility and threat awareness.

Next, we're all aware of the work toward the establishment of international norms for behavior in cyberspace. There has been a lot of great work in that area so far, such as Christopher Painter's work at the State Department, and private groups such as the Digital Equilibrium Project, just to cite a few examples. This is an area where the U.S. and its allies must continue to push, through direct engagement and in international fora. A critical aspect of this must be respect for financial and economic integrity.

Beyond information sharing and bounding egregious behavior is coordinated defense. Once we have sufficient international shared visibility to identify major threats, the next step is coordinating multi-nation responses to them. A simple example would be large distributed denial of service (DDoS) attacks. The sources that contribute to such attacks are frequently distributed across several countries. Coordinated response can shut down these attacks more effectively than piecemeal efforts, and act as a more effective deterrent against threat actors who use them. Creating the mechanisms and practices for internationally coordinated defense will be hard, but we can start small. The U.S. might choose to start with our FVEYS partners, building on the many areas of where we already cooperate.

The U.S. and its allies, together, can drive the international agenda for enhancing key aspects of global cybersecurity. We should seize that opportunity.

*Workforce and Preparing for the Long Term*

Many of the areas I've described in this statement are about technical measures we can take to improve our contemporary cybersecurity posture. But how can we create conditions for long-term success? How can we prepare for sustaining confidence as cyberspace continues to grow and change?

We lack sufficient workforce to fill cybersecurity and defense roles. The shortage will continue indefinitely unless we take action to alleviate it. Automation will help some, by increasing defenders' scope and efficiency. I believe we need to pursue three parallel lines of effort:

- Build up educational capacity in cyberspace areas, with emphasis on security and defense
- Support students pursing degrees and certificates in these areas, both directly through scholarships, and indirectly through internship programs and industry incentives. (The NSF Cybercorps Scholarship for Service program, for example, has been very successful in drawing talented undergraduates and graduate students into cybersecurity, and then placing them in government positions at the start of their careers).
- Extend education in cybersecurity basics down to a secondary school level. The best mechanism for this, so far, has been education for teachers, but competitions and summer programs for students have also been effective at small scales.

I've been involved in NSA's efforts to foster information assurance and cyber defense education since about 2003, and together with DHS, we have made a difference- the U.S. now has a solid base from which to build. But the current programs are very small. We can do more from government, and even better we need to get the private sector more involved in supporting students and building capacity.

Preparing the workforce for tomorrow's challenges is a long-term investment, but one that will yield sustained return for the digital economy.

Besides the core foundation of the workforce, future cybersecurity also depends on vital and innovative research and development community. The U.S. is in pretty good shape on the development side; we've had many nimble companies and investors to support them. But they depend on a steady stream of new ideas and innovative researchers. The primary source for those are our research universities. Student support must extend up to the doctoral level, because those graduates are the next generation of research leaders and professors. Direct research funding is always good, but government may be able to create greater impact by facilitating tech transfer. Therefore, I recommend setting up a program for improving dissemination of government-funded cybersecurity research results, and encouraging industry to take advantage of it.

The U.S. has a strong foundation in education and research for cybersecurity. If we can leverage it, we can sustain technological leadership in this critical area, and be better prepared for future cybersecurity challenges.

## **Conclusions**

I've outlined a few of the challenges I think are most important to address in the current cybersecurity environment. None of them are unsurmountable. We have the base necessary to address them, both in the public and private sectors, we need to apply some focused efforts.

- Promote security improvements in commercial products and services by setting standards, testing against them, and driving use of products that pass
- Drive conscious assessment and management of risk, through use of well-structured frameworks
- Harden foundational services that support secure activity in cyberspace, especially the domain name service, services for identity, and Internet routing
- Aggressively advance information sharing, through automated means, through both technical and policy mechanisms
- Build the fundamentals for shared defense, including technical standards for orchestrated response and practices for executing it
- Continue to bolster the ecosystem for trustworthy identity, and standardizing the means for secure attribute assertions. Government must lead by example in this space
- Extend information sharing across international allies, to create broader visibility of cyberspace activity, and the basis for coordinated international response for cyber attacks
- Build up educational capacity and support students pursuing an education in cybersecurity
- Sustain national cybersecurity research capacity, and promote transfer of research results to the market

By undertaking these measures, I believe that the U.S. can create the confidence that is essential for growing the digital economy.