International Cybersecurity Priorities:
Fostering Cybersecurity Innovation Globally
U.S. Department of Commerce
June 26, 2017

Executive Summary

The U.S. Department of Commerce's goals of ensuring that technology products and global networks are interoperable, resilient, and secure is essential not only to U.S national security interests, but also to continued U.S. economic leadership. Global trust in the Internet and confidence in the security and stability of the platforms and services that comprise this highly diverse ecosystem is vital for U.S. industry.

Presidential Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* instructs the Secretary of Commerce to submit, within 45 days, "a report to the President on the international cybersecurity priorities of the Department, including those concerning investigation, attribution, cyber threat information sharing, response, capacity building, and cooperation."

This paper, *International Cybersecurity Priorities: Fostering Cybersecurity Innovation Globally* articulates the Department of Commerce's general approach towards cybersecurity policy, and, consistent with that approach, identifies the Department's various priorities in international engagement. Those priority areas can broadly be categorized into five overarching themes:

I. **Encouraging and facilitating cybersecurity innovation through the global marketplace**
II. **Ensuring cybersecurity approaches and policies are globally relevant**
III. **Advocating for US cybersecurity products and services internationally**
IV. **Enhancing global Internet security and stability**
V. **Building international capacity on cybersecurity education and workforce**

This report emphasizes the importance to the U.S. economy of a continued focus on advancing standards-based, industry-led consensus cybersecurity solutions and innovation. It advocates for sustained, significantly expanded, international engagement on cybersecurity and information and communications technology (ICT) issues.

Specifically, the report recommends the following to inform an international strategy in order to further the priorities listed above:

- Continue to advocate internationally for industry-led and consensus-based cybersecurity standards and effective, voluntary solutions;

- Prioritize international market access for U.S. cybersecurity companies – including providers of cybersecurity products and services – and combat trade barriers;

- Advocate that intergovernmental organizations outputs should not include prescriptive text calling for global cybersecurity legal frameworks or cybersecurity treaties, to ensure cybersecurity solutions remain flexible;
- Focus on the international adoption of cryptographic technologies;
- Expand international participation in multistakeholder processes with international partners;
- Leverage cybersecurity educational initiatives to build capacity among key partners and show American leadership internationally.

The modern economy can fully thrive only when businesses and consumers alike can trust the security and privacy of their networks, systems, and applications. The Department works determinedly across its agencies and bureaus, engaging collaboratively with the owners and operators of the digital infrastructure, to enhance the security and resiliency of the ecosystem. As the voice of U.S. industry, innovation, and competitiveness within the U.S. government, the Department is poised to continue to shape the policies, initiatives, and strategies necessary to ensure national cybersecurity priorities and continued U.S. leadership across the Internet ecosystem.

International Cybersecurity Priorities:
Fostering Cybersecurity Innovation Globally

Cybersecurity at the Department of Commerce

Technological innovation has transformed the economic and social fabric of the United States and the world. Digital technologies have quickly become a key driver of jobs, business creation, and innovation in the 21st century. Economic growth and competitiveness depend fundamentally upon a nation's ability to harness the transformative opportunities of the Internet, computers, and information. Nearly all industry sectors, from manufacturing to financial services, education, agriculture and health care, have benefited from the adoption of digital technologies, applications, and services.

As the voice of U.S. industry, innovation, and competitiveness within the U.S. government, the U.S. Department of Commerce plays a leading role in helping to shape the various policies, initiatives, and strategies necessary to ensure continued U.S. technological leadership. However, the growth and maturation of the use of information technology has been accompanied by a parallel growth and intensification of risks to these systems and networks. These risks include indiscriminate and broad-based cyberattacks from malicious actors that seek to steal, manipulate, destroy, or deny access to sensitive data, or to disrupt critical infrastructure.

It has become clear that the economy can only fully thrive when businesses and consumers alike can trust the security and privacy of their networks, systems, and applications. But these mounting threats not only affect individual firms and their customers, they also pose a persistent economic and national security challenge to the nation. Effectively securing digital systems is therefore essential not only to the success of individual companies and the security of individual users, but also to the basic functioning and vitality of our economy and our society.

With this in mind, the Department works determinedly across its agencies and bureaus to enhance the security and resiliency of the digital ecosystem. It aims to improve digital security across the economy without stifling innovation or growth; it seeks to develop innovative security solutions that both protect and enhance the free and open Internet; and it looks to give industry a leading voice in setting the technical standards needed to protect systems and users alike.

Diverse Cybersecurity Expertise

The Department of Commerce is composed of 12 bureaus and nearly 47,000 employees, located in all 50 states and territories, and in more than 86 countries worldwide. Although the bureaus have vastly different mandates and specializations, they work in concert to create an enabling environment for American industry, including through the development of cybersecurity innovation, education, and guidelines. The Department seeks to complement, not duplicate, the efforts other federal and private sector entities. It does this leveraging the unique technical expertise of the women and men who staff the Department's many cybersecurity programming offices, research laboratories, and policy shops, both domestically and in U.S. embassies.

The ***National Institute of Standards and Technology (NIST)*** develops technical standards and guidelines for securing non-national security federal information systems, and works with industry and other agencies to define security requirements for federally-held information and information systems. These are often important guides for the private sector, both for critical and non-critical industry sectors. In addition, NIST leads and contributes to standards development work in a wide range of domestic and international standards bodies, evaluates private sector security policies for potential federal agency use, and provides general cybersecurity technical support and assistance to the private sector and federal agencies. NIST standards, guidelines, and recommendations for cybersecurity include specific technical implementations of cryptography, enterprise risk management strategies, and applied cybersecurity engineering best practices. The Director of NIST serves as the President's principal adviser on standards policy pertaining to the Nation's technological competitiveness and innovation ability.

The ***National Telecommunications and Information Administration (NTIA)***, in its role as principal adviser to the President on telecommunications and information policies, works to protect the Internet's core networking infrastructure, such as the Domain Name System (DNS), to support secure broadband deployment across the United States, and to assist with the development of cybersecurity best practices, among other issues. As an advocate for digital innovation, NTIA has played an instrumental role in developing policies that have helped expand and secure the Internet and the broader digital ecosystem over the past several decades.

The ***International Trade Administration (ITA)*** leads the Department's export and investment activities and ensures fair trade through the rigorous promotion and defense of trade laws and agreements, including those relevant to cybersecurity products and services. As the premier resource for American companies competing in the global marketplace, with more than 2,200 employees assisting U.S. exporters in more than 100 U.S. cities and 75 markets worldwide, ITA helps to promote global leadership of U.S. companies in the ICT sector and to facilitate overseas partnerships that better position the United States to benefit from overseas cybersecurity business opportunities.

The ***Bureau of Industry and Security (BIS)*** works to advance U.S. national security, foreign policy goals, and economic growth by ensuring an effective export control and treaty compliance system, and by promoting continued U.S. strategic technology leadership. In the case of dual-use technologies, such as cryptographic and cybersecurity software and technology that could be abused by malicious actors or hostile governments, the Bureau vigorously administers and enforces export control rules to keep such tools out of the hands of untrustworthy parties. In furtherance of this mission, BIS seeks to avoid imposing unreasonable restrictions on legitimate international commercial activity that is necessary for the health of U.S. the American technology industry, or unduly compromise the international competitiveness of U.S. industry.

In addition, several other agencies and bureaus of the Department play a more limited, though still substantive, role in advancing American cybersecurity interests. These include **the *United States Patent and Trademark Office (USPTO)***, which promotes innovation domestically and abroad by helping Americans protect and enforce their patents, trade secrets, trademarks, and copyright, and advocating for stronger intellectual property policies around the world, the ***Economics & Statistics Administration (ESA)***, staffed by economists and statisticians who conduct research and analysis on a variety of digital economy issues, and the ***National Oceanic and Atmospheric Administration (NOAA)***, which develops and deploys information security systems for its many scientific resources, such as its weather satellites.

These agencies and bureaus all play a part in protecting our digital world. Indeed, the underlying strength of the Department is the ability of its various agencies and bureaus to collaborate and share their particular technical expertise. What unites the bureaus and agencies of the Department is a shared commitment to fostering and promulgating innovative, reliable, and growth-enabling cybersecurity solutions across the United States and around the world.

Key Commerce International Cybersecurity Initiatives

Cybersecurity Framework – The NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) is a comprehensive guide to help organizations manage cybersecurity risks. Created as a collaboration between the U.S. government and the private sector, the Framework uses a common language based on international standards to address and manage cybersecurity risk in a cost-effective way based on business needs, without placing additional regulatory requirements on businesses. Foreign governments and private firms alike are using the Framework to improve their cybersecurity risk management efforts.

NTIA Cybersecurity Multistakeholder Processes – NTIA utilizes “multistakeholder” policymaking on a range of global cybersecurity policy issues, recently including vulnerability research disclosure and IoT security upgradability and patching. Multistakeholder processes involve parties from across the global digital ecosystem interested in a specific policy challenge, working together in an open, transparent, and consensus-driven manner, to develop flexible and innovative solutions to their mutual benefit. NTIA’s processes have led to the development of options, best practices, specifications and sample policies for improving cybersecurity collaboration across the ecosystem.

Interagency and Stakeholder Engagement to Protect a Vibrant and Open Internet – An open, stable and secure Internet has led to unprecedented innovation and economic advancement but protecting this global infrastructure requires consistent and targeted collaboration with infrastructure owners and operators, as well as government stakeholders focused on minimizing national security risks. The Department of Commerce is the leading voice on promoting voluntary best practices and standards adoption, while also working with government stakeholders on approaches to national security threats that protect the resilient characteristics of the infrastructure.

NIST Cybersecurity Standards Development and Coordination - NIST leads the U.S. government in the research, development, deployment, and promulgation of the highest quality and most trustworthy cybersecurity standards, guidelines, tests, and metrics. Internationally, the technical experts of NIST participate in a range of global standards-setting bodies where they advocate for cybersecurity standards that are technologist-driven and developed in an open, transparent, traceable, and consensus-based manner.

Cybersecurity Workforce Development -- Cybersecurity education and workforce development programs are at the core of the Department's mission. A strong cybersecurity workforce is critical to continuing U.S. leadership in the digital economy. The security of U.S. networks is inexorably tied to the security of devices and systems overseas. Thus, ensuring cooperation on international cybersecurity workforce development and education is essential.

Priority I – Encouraging and facilitating cybersecurity innovation through the global marketplace

The technology and services that keep the global digital ecosystem trustworthy and thriving depend on the marketplace. A range of solutions are needed to support this ecosystem, including traditional products like antivirus and firewalls; services to monitor networks against advanced attacks; and increasingly, more secure consumer products. The path towards improved security depends on new ideas, collaboration across sectors to develop these ideas, and active competition between potential solutions to drive better solutions into the global market. These solutions cannot be national solutions – they must work for a global marketplace. It is important to incentivize international markets, technologies, services and companies that provide these ideas and innovations in security.

Security solutions must constantly evolve as threats evolve. This evolution requires an active market-based ecosystem. Threats are discovered by researchers, solutions are developed by top companies, elite companies are early adopters, and over time these solutions are integrated into the existing marketplace and become part of how organizations and citizens defend themselves. This marketplace does not always function perfectly. We do not have a clear idea of how the threats will evolve, or exactly what kind of contribution individual tools have to the overall security of an organization. At this time, there is no easy path to understand the 'return on investment' for security.

This is one of the reasons why the Department of Commerce plays a key role in advocating the development of international standards for cybersecurity, with a focus on interoperability, security, usability, and resilience. These characteristics improve trust in online and offline transactions and promote innovation and competitiveness, thus enabling organizations to more easily and effectively integrate new technologies and services, and helping U.S. products and services to more competitively enter in global markets. Increased, more strategic and better-coordinated U.S. engagement in cybersecurity standardization internationally will help to further promote U.S. interests by ensuring that standards-based requirements for cybersecurity products, processes, and services further U.S. interests and that standards are not used as technical barriers to trade.

For information on the Department's specific programs under this priority, see the Appendix.

Priority II – Ensuring cybersecurity approaches and policies are globally relevant

U.S organizations can compete internationally when commonly known and understood best practices and policies are adopted globally. Considerable effort is spent ensuring opportunity abroad by ensuring U.S. cybersecurity approaches and policies are globally relevant, and then socializing those approaches and policies in way to maximize international use. This sets the stage for U.S. cybersecurity products and services to compete abroad (Priority III).

One challenge is that there is no one-size-fits all fix to many of these challenges. Different organizations, with different values at risk, face different threats, and have different approaches to dealing with them. Good practices and policies reflect this diversity, and help firms understand what solutions will work for them. In the global marketplace, an organization may have much more in common with a similar firm in a different country than the company across the street. The Department accordingly develops and promotes tools that enable organizations around the world to deal with the threats they face.

The digital marketplace is a global marketplace. The nature of cyberspace allows information to flow at the speed of light, and connect citizens and businesses around the world. Moreover, the physical technology and the services that support it are also part of a global market of trade and supply chains. While each country may have its own cybersecurity strategy, the policies and practices that they use to implement that strategy will apply to systems that, optimally, are standardized and interoperable with the rest of the digital ecosystem. Attempts to create global legal frameworks and country-specific rules or practices can undermine the innovation that supports the global IT industry. Disrupting the global nature of this market not only threatens free trade of those goods and services, it risks all the innovation and growth that sits atop a digital platform of shared data and services.

The global nature of modern supply chains also poses new security threats. Attackers have used corporate partners and the upstream and downstream suppliers to compromise networks and wreak digital havoc. U.S. organizations need to work with their partners to help them be secure, and maintain the integrity of their supply chains. This requires a common, global understanding of risk, and policies and practices that will have impact around the world.

Priority Markets

The Department of Commerce has a network of digital trade officers located in strategic markets tasked with helping cybersecurity exporters, along with other digital products and services exporters, gain market access and navigate foreign digital policy and regulatory issues. These Digital Trade Officers are currently found in the following countries: *Belgium, Brazil, China, France, Germany, India, Indonesia, Japan, Mexico, Singapore, South Africa, and South Korea*

For information on the Department's specific programs under this priority, see the Appendix.

Priority III – Advocating for U.S. cybersecurity products and services internationally

The cybersecurity companies of the United States are the most cutting-edge cybersecurity providers in the world. Whether it is cybersecurity products, such as network-monitoring systems or firewalls, or cybersecurity services, such as security testing and audits or cyber risk consulting, the technology providers of the United States are the world's leaders in enterprise and consumer cybersecurity solutions. This is why U.S. cybersecurity products and services are continually in high demand overseas and why the Department of Commerce is focused on promoting U.S. cybersecurity exports around the world. U.S. IT companies are continuing to build products that are more inherently secure, safe and resilient. While we look to cybersecurity markets to assist, the long-term solutions will come from the IT products that are designed, built, configured and deployed with security requirements native in those products.

This is especially the case because cybersecurity is a rapidly growing industry globally. It is estimated that worldwide spending on cybersecurity products and services topped $81.6 billion in 2016, an increase of 7.9 percent over 2015, and could continue to grow at a rate of 5-10 percent annually through 2020.[1] According to market analysts, while North America and Europe remain at the top of cybersecurity spending today, the Asia-Pacific region, driven by emerging economies such as China, is quickly becoming a lucrative market for cybersecurity providers. India, likewise, is expected to see significant growth in the cybersecurity spending over the next decade,[2] with the country's cybersecurity market projected to grow nine-fold to $35 billion by 2025, from about $4 billion today. And while South America and Africa continue to lag behind more economically-developed regions, they are quickly increasingly their overall spending on cybersecurity products and services as well.

[1] Gartner 2016 Report.

[2] https://www.dsci.in/content/growing-cyber-security-industry-roadmap-india

The Department of Commerce, and in particular the International Trade Administration (ITA), serves as advocates for the U.S. tech industry around the world. They do this by supporting U.S. commercial trade missions and other trade promotion activities. Perhaps even more importantly, they do this by vigorously encouraging the kinds of legal, policy, and investment climates around the world that are conducive to a robust and global U.S. cybersecurity market. Critically, this policy advocacy includes the promotion of cross border data flows, which is not only important for the continued vitality of the global Internet, but also for ensuring that global companies, of all kinds, can track cybersecurity incidents and coordinate defenses to cyber-attacks. In addition, given the high correlation between unlicensed or pirated software and cybersecurity threats, the Department's ongoing efforts to educate consumers and to advocate for measures to combat software piracy contribute to overall security in the digital environment.[3] The Department intends to amplify this trade promotion and policy advocacy over the coming years. The Department intends to amplify this trade promotion and policy advocacy over the coming years.

For information on the Department's specific programs under this priority, see the Appendix.

Priority IV – Enhancing global Internet security and stability

Internet technologies provide a technical basis for most systems vital to our nation, including communications networks, transportation, manufacturing, defense, and education. The security and stability of the public Internet, and private networks that are based upon Internet technologies, are threatened by the vulnerabilities that are inherent in many of the core infrastructural protocols in use today. Given the complexity and scale of the Internet, and the sophistication of adversaries that attempt to subvert the networks and protocols it depends on, it is vital that we engage the industry and international partners to develop and promulgate solutions to these cybersecurity issues.

The Department advances critical Internet related security worldwide by fostering the development and adoption of technologies which; (1) increase the security and stability of a number of core infrastructural Internet technologies, including the global naming and routing systems (e.g., the Domain Name System and the Border Gateway Protocol); (2) enhance the security of Internet hosts (e.g., hardware roots of trust) and online applications (e.g., Transport Layer Security); and (3) establish interoperable security primitives such as cryptographic functions. To achieve this, the Department works in collaboration with all stakeholders in the creation of voluntary and vendor-neutral security standards, frameworks, and architectures. It also sponsors and participates in cutting-edge security-focused technical development that draws on the expertise of industry, academia, and other experts from around the world.

The Department recognizes that success in addressing the Internet security and stability challenges depends on our ability to leverage not only its world-class technical and scientific

[3] There is a high correlation between unlicensed or pirated software and cybersecurity threats. *See*, IDC White Paper Unlicensed Software and Cybersecurity Threats, ***http://globalstudy.bsa.org/2013/Malware/study_malware_en.pdf***

expertise, but also the expertise and experience of subject matter experts in industry and academia, and other interested researchers. The Department's working groups are open to all interested parties, with results freely available to all stakeholders in the commercial, academic, and government sectors.

In every related activity, the Department undertakes or participates in, international stakeholders are consulted and engaged in order to advance our common goal: the security and stability of the Internet worldwide. With its emphasis on technical excellence, involvement of all interested stakeholders, and the availability and relevance of its outputs to all, the Department of Commerce will continue to advance Internet security and stability both directly and through its support for the kind of innovation that will generate the security measures of the future.

For information on the Department's specific programs under this priority, see the Appendix.

Priority V – Building international capacity on cybersecurity education and workforce

One of the most important ways we protect our systems from cyber risks is through the development of a well-educated and well-trained cybersecurity workforce. Cybersecurity education and workforce development programs are at the core of the Department's mission. It is critical to continuing American leadership in science and technology. However, as has been noted throughout this report, the digital economy is globally interdependent. The security of American networks is inexorably tied to the security of devices and systems overseas. Weaknesses in devices and systems overseas present a very real and persistent risk to devices and systems domestically.

To assist this challenge cybersecurity education and workforce development overseas is a focus of the Department. Foreign partners are eager to learn from the Department's experience leading cybersecurity education programs, such as NIST's National Initiative for Cybersecurity Education (NICE). The Department intends to expand its education and workforce development efforts overseas, both to build capacity among key partners, but also as a means of showing American leadership internationally on a critical component of the cybersecurity challenge.

For information on the Department's specific programs under this priority, see the Appendix.

Conclusion: Key Recommendations for International Engagement

The Department of Commerce recommends the following to inform an international strategy in order to further the priorities listed above.

- Continue to advocate internationally for industry-led and consensus-based cybersecurity standards and effective, voluntary solutions.
    - Promote the NIST Cybersecurity Framework

  - Leverage Department technical expertise to develop and shape US government proposals and responses to cybersecurity standards related proposals being considered within international organizations, such as the ITU, the G-20, and G-7
  - Analyze cybersecurity standards for IoT hardware, software, and applications, and develop priorities for IoT cybersecurity standards engagement – including identifying new standards work items and preferred international venues for developing those standards
  - Explore voluntary practices for market-based IoT security solutions and share those practices internationally
  - Continue to advocate for measures to effectively combat software piracy and other illegal activities that threaten the digital infrastructure

- Advocate that intergovernmental organizations outputs should not include prescriptive text calling for global cybersecurity legal frameworks or cybersecurity treaties, in line with the Department's emphasis on keeping cybersecurity solutions flexible

- Focus on the international adoption of cryptographic technologies used throughout the Internet, including DNSSEC, IPSEC, BGPSEC, TLS, and others
  - Promote IPv6 adoption and use and secure inter-domain routing
  - Build international coalitions in support of the KSK rollover process

- Prioritize international market access for U.S. cybersecurity companies – including providers of cybersecurity products and services – and combat trade barriers through:

  - Facilitating global data flows and combat data localization measures
  - Focusing on inclusion of cybersecurity provisions in trade agreements
  - Continuing to implement the EU-U.S. and Swiss –U.S. Privacy Shield Frameworks
  - Continuing to implement and expand the APEC Cross Border Privacy Rules (CBPR) System

- Expand international participation in multistakeholder processes and share process results with international partners

- Share the Department cybersecurity educational initiatives to show how these approaches can scale internationally to assist in fulfilling workforce gaps in other countries

APPENDIX - DEPARTMENT OF COMMERCE: PRIORITY PROGRAMS IN CYBERSECURITY

Priority I - Encouraging and facilitating cybersecurity innovation through the global marketplace

Standards Advocacy

Voluntary consensus standards are an important tool that can help achieve the priority that cybersecurity policies and practices are globally relevant. Cybersecurity related voluntary consensus standards that are developed in open, transparent, consensus-based manner in private-sector organizations, and are industry-led and market-relevant can help minimize the risk of standards being used as technical barriers to trade, while helping create an environment that can foster innovation and competition.

Federal agencies participation in the development and use of standards is guided by a range of statutory and policy tools. The National Technology Transfer and Advancement Act of 1995 (PL 104-113) mandates that all federal agencies use technical standards developed and adopted by voluntary consensus standards bodies, in lieu of using government unique standards. The Office of Management and Budget (OMB) Circular A-119 (most recently revised in 2016) provides federal agencies guidance on how federal agencies can participate in the development of such standards, and how they can use voluntary consensus standards to further their agencies' mission. The foundation established by these two policy tools have led to a very strong public-private partnership for standards development and use, in the U.S. With the private sector and federal agencies bringing together their respective strengths, the U.S. has continued to be effective in leading the development of timely and robust standards, including those for cybersecurity.

Effective, timely and robust standards through participation of NIST technical experts in development of international standards resulted in adoption of the NIST driven or coordinated technology for block ciphers, authenticated encryption, hash functions, digital signatures (e.g., in ISO-IEC/JTC1/SC27). NIST staff's participation[4] in organizations such as 3GPP, Bluetooth Special Interest Group, the FIDO Alliance, IEEE 802, IETF, ISO-IEC/JTC1/SC17, ISO-IEC/JTC1/SC 38, ISA, TCG, X9, and others is ensuring that US government and the Department's interests are reflected in the standards being developed in these organizations covering a wide range of technologies such as mobile telephony, short-range wireless communications, financial information and transactions, instrumentation, and identities.

NTIA Vulnerability Disclosure Multistakeholder Process

In 2015, NTIA launched a multistakeholder process to promote collaboration around the disclosure of security vulnerabilities. There is widespread recognition that information

[4] https://www.nist.gov/sites/default/files/documents/2017/05/15/ITLVolStdsList.pdf

technology systems - from traditional software to popular websites and cloud platforms to embedded devices - will never be completely secure. It is inevitable that vulnerabilities will be discovered, as a key aspect of security research as well as an integral part of the burgeoning security industry. This issue has been long debated, but the increasing dependence on software, and the growth of the security research community has made the need for collaboration more urgent. The goals of the NTIA process sought to expand the 'norms' of collaboration around vulnerabilities, increasing the number and type of companies that are interested and capable of working with researchers, and help researchers understand how to work with companies around the globe.

Stakeholders in this process included a wide range of security researchers, security companies, and software companies, and representatives from a range of industries, including retail, auto, and medical device manufacturers. Many stakeholders came from companies based overseas, and even more companies explicitly worked from the assumption that they were addressing an international marketplace. They produced three important documents: a survey and study of researcher motivation to better support collaboration; a template disclosure policy to help organizations begin to work with the security research community, with a special focus on safety-critical industries; and a framework to help advanced technical players work together when a disclosure requires multiple parties coordinate their actions to address a vulnerability. More broadly, stakeholders and NTIA have worked to normalize the process of vulnerability disclosure, and worked with international colleagues to make it a more common, accepted part of dealing with security risk internationally.

National Vulnerability Database (NVD)

NIST runs the National Vulnerability Database (NVD), as a U.S. government repository of vulnerability management data that is shared openly. The database integrates publicly available U.S. government vulnerability resources and provides references to industry resources. The critical role that the NVD plays is evident in the fact that most major cybersecurity software, such as anti-virus software, query the database for known vulnerabilities. The success of the NVD is integrally dependent on the strong public-private partnership that exists between NIST, U.S. Government agencies, academia and the international information security industry.

NTIA Internet of Things Security Upgradability Process

Security is one of the most common concerns around the growth of the Internet of Things (IoT). However, broad guidance often lacks the potential to drive action. NTIA has worked on one particular area of concern: addressing potential security vulnerabilities in IoT devices or applications through patching and security upgrades. In the early IoT market, there has sometimes been limited consideration for supporting future security patches, even though many devices will eventually need them. An approach focused only on government policies would not work alone, given that many of these products are developed and manufactured overseas.

Enabling a thriving global market for devices that support security upgrades requires common principles and definitions so consumers know what they are getting, and manufacturers have some incentives to build out update capabilities.

Stakeholders and NTIA are working to move forward in the IoT security discussion by shaping a broad consensus around the importance of patching IoT devices and the tools to support this approach. Stakeholders in this process recognized that this issue has both technical and policy components. On the technical side, they are working to map out the necessary steps in a security update, and what the minimum features for those updates might be; they are also reviewing existing IoT technical standards to assess the state-of-the-art, and extract lessons that can be used by future initiatives. On the policy level, stakeholders have proposed a simple, easy-to-understand set of elements that manufacturers around the world can use to communicate to consumers prior to purchase. The final approach stakeholders have taken is to study the incentives and barriers for patching across the ecosystem, trying to move beyond the axiom that "no one will pay for security." As with all its domestic cybersecurity work, stakeholders were explicit that this is not a purely domestic problem, and NTIA and its stakeholders plan to evangelize this framework internationally as part of its various international engagements.

Cryptographic Technology Standards and Product Assurance

NIST conducts research, development and engineering in cryptographic algorithms, methods and protocols. NIST produces standards, guidelines and reference material for the design, use and implementation of cryptography for organizations of all sizes, for industry and for international implementations. NIST's cryptographic work is built into commercial products and used by the U.S. Government, industry and worldwide to protect information and systems.

A strategic area of concern for markets is the balance of industries, markets, and nations to minimize risks in the use of cybersecurity technologies through conformity assessment. Conformity assessment enables buyers, sellers, consumers, and regulators to have confidence that products sourced in the global market meet specific requirements. It is the demonstration that specified requirements relating to a product, process, system, etc. are fulfilled. Conformity assessment activities form a vital link between standards (which define necessary characteristics or requirements) and the products themselves. Conformity assessment procedures provide a means of ensuring that the products, services, and systems have certain required characteristics, and that these characteristics are consistent from product to product, service to service, system to system, and so on. Conformity assessment can include: supplier's declaration of conformity, sampling and testing, inspection, certification, management system assessment and registration, the accreditation of the competence of those activities, and recognition of an accreditation program's capability. Standards are interwoven into all aspects of these activities and can have a major impact on the outcome of a conformity assessment scheme or program.

NIST's experts work to ensure that product assurance activities are built on standards and conformance approaches that leverage testing programs that leverage existing frameworks and private sector expertise, are international, are mutually acceptable, protect product and embedded intellectual property and are not used as trade barriers. The NIST Cryptographic Module Validation Program is one example of an approach where vendors of cryptographic modules use independent, accredited laboratories to test their modules and generate confidence for use by US government agencies to protect sensitive information.

NIST Security for IoT

The NIST Security for IoT program is based on work with stakeholders across industry, academia, international bodies and government, to cultivate trust in the Internet of Things and to promote U.S. leadership in IoT through standards, guidance, and related tools. The program focuses on fundamental and applied research leading to the transfer of these to industry to enable technology advances and innovation. Active work is ongoing in fundamental research, including standards and guidance that address security for IoT in areas such as: Lightweight Encryption, which provides basic security cryptographic capability to small, sensor based products; RFID and Bluetooth Security to assure the data transmitted by IOT devices can be done securely and with assurance; BIOS Integrity allows for security of firmware and basic chip instructions often used in IOT devices; Industrial Control Systems Security is needed for industrial IOT and large scale implementations that might not have the same missions or constraints of other IOT use cases.

Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework)

In 2014, NIST issued the Framework for Improving Critical Infrastructure Cybersecurity (Framework). The Framework, created through collaboration with industry, government, and academia, consists of international standards and practices to promote cybersecurity risk management. Since its release, NIST has strengthened its collaborations with critical infrastructure owners and operators, industry leaders, government partners, and other stakeholders to raise awareness; encouraged use of the Framework by organizations supporting the critical infrastructure; and developed implementation guides and resources, all of which contribute to reducing cyber risks to U.S. critical infrastructure. And while the Framework was borne through U.S. policy, it is not a "U.S. only" framework; many countries and international entities are adopting an approach that is compatible with the Framework. Today, a host of organizations, both domestically and overseas, have added services and products for Framework-based assessments of organizations their suppliers. Additionally, most audit and consulting firms have leveraged the Framework for their own cybersecurity assessment programs.

Trusted Identities

NIST is working to advance measurement science, technology, and standards adoption to improve digital identity for individuals and organizations alike. As called for in the

Cybersecurity Enhancement Act of 2014, the NIST works with its partners to drive trust, convenience, and innovation in the marketplace of identity solutions. NIST aims to promote a private sector-led approach to advance trusted digital identity solutions that can scale globally, while enabling government adoption by continually evolving international standards and our risk-based federal guidance to encourage the adoption of innovative technologies available in the market.

Software Assurance, Testing and Secure Design Standards

NIST works with industry, academia and standards bodies to accelerate the development and adoption of correct, reliable, testable software, leading to increased trust and confidence in deployed software. NIST also: promulgates methods to develop better standards and testing tools for today's software infrastructures and tomorrow's next-generation software systems; advances the state of the art of software testing by developing scientifically rigorous, breakthrough techniques; and leads efforts for conformance testing, especially at the early stage of standards development. Lastly, NIST develops integrated test environments to coalesce systems and facilitates the transfer of these activities and technologies into national infrastructures and commercial sectors.

USPTO Cybersecurity Partnership Meetings

The United States Patent and Trademark Office (USPTO) hosts Cybersecurity Partnership Meetings in Silicon Valley, California. The meetings serve as a collaborative forum for stakeholders seeking patent protection in the cybersecurity and network security sectors to share ideas, experiences, and insights with USPTO staff.

Priority II - Ensuring cybersecurity approaches and policies are globally relevant

Interagency International Cybersecurity Standardization Working Group

The Interagency International Cybersecurity Standardization Working Group (IICSWG) coordinates on major issues in international cybersecurity standardization across the U.S. government and enhances U.S. federal agency participation in international cybersecurity standardization. The IICSWG is currently working to determine the current state of international cybersecurity standards development for the Internet of Things. This information will be available to assist each agency in its planning for IoT and will help to coordinate the overall U.S. government participation in such activities.

In 2015, NIST, on behalf of the Federal Government's International Cybersecurity Standardization Working Group (IICSWG) issued an Interagency Report on "Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity." [5] This report laid out the imperatives for enhancing U.S. government

[5] http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v1.pdf

coordination and participation in the development and use of international standards for cybersecurity, and included recommendations on how these objectives could be met. This report was accompanied by a supplemental report[6] that summarized ongoing federal engagement in international cybersecurity standardization, the landscape of standards organizations, and included information federal agencies could leverage to more effectively engage in international cybersecurity standards development.

The reports and the IICSWG contribute to the federal government's approach to meeting cybersecurity-related requirements. Furthermore, this approach also provides both US government and US industry an additional means to articulate and champion the US approach to standards that is private-sector led, industry-driven approach with government participation, and that emphasizes the use of international standards developed in open, transparent and consensus-based processes. This approach allows both US private sector companies (in collaboration and independent of each other) to engage with foreign government officials (e.g., from China, Japan, the European Commission, India) to highlight the openness and transparency of the US government's approach, while simultaneous pressing government representatives to adopt a similar path. While only focused on cybersecurity issues, the approach of the IICSWG could be a model for effective federal government engagement on other challenges pertaining to international standards bodies.

The Wassenaar Arrangement

An area of emerging international cooperation in cybersecurity regulation is multilateral export control. However, while export control can play an important role, it is critical that efforts to regulate cyber-related software and technology in the global environment carefully balance potential benefits against potential harm to critical cyber defensive activities.

In 2013, the 41-member Wassenaar Arrangement adopted controls on the export of certain cybersecurity products and technology that have a dual-use, including deployment and control of network intrusion software.[7] These controls were proposed to target a narrow range of specific products for human rights purposes (e.g., surveillance of dissidents), although products/technology can be used for a variety of nefarious purposes.[8] After extensive stakeholder opposition to a proposed US rule implementing these controls, it became clear that the language originally adopted would materially harm defensive analysis, cooperation and incident response. As a result, the US has returned to Wassenaar to work for improvements. BIS, in cooperation with State, Defense, and DHS, will continue to carefully vet the increasing number of control proposals relevant to cyber emerging from Wassenaar to ensure that they do

[6] http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf

[7] BIS citation

[8] BIS citation

not impede international cyber cooperation and do not disadvantage US products, services, and cyber defense.

NIST CSF International Advocacy

Industry stakeholders have repeatedly highlighted the importance for the Department to engage internationally to insure other countries take approaches that can be aligned to the Cybersecurity Framework. This alignment helps stakeholders reduce the burden of international regulatory and legal regimes, leading to a reduced cost of operation and a greater understanding of international policies. It also highlights the value of a bottoms-up approach for other governments and they develop their cybersecurity priorities.

NIST's approach to achieving this alignment is multi-pronged. A short-term effect is achieved by direct discussions with foreign governments to encourage their endorsement of CSF or publication of complimentary national frameworks. To date, NIST has engaged directly with more than 30 foreign governments regarding the CSF. One tangible result of this effort is Italy's publication of their National Framework for Cyber Security, which is based entirely on the CSF.

A longer-term, yet broadly affecting, approach is also underway on international CSF use. NIST is working with the American National Standards Institute (ANSI) the U.S. member body to the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to develop international standards aligned with CSF to develop international standards aligned with CSF. Joint working groups of ISO and IEC have launched studies on the relevance of CSF to ISO/IEC standards. The anticipated conclusion of this work will likely put CSF on a path to becoming an ISO/IEC Technical Specification. This has a broad and positive effect, because of extensive use of ISO/IEC standards. It also has a positive effect for nations that are looking for approaches based more directly on international standards.

FISMA International Advocacy

NIST develops a suite of Risk Management Guidance in accordance to The NIST Act and the Federal Information Security Management Act. This requires NIST to develop standards and guidelines for US Government information systems. As part of this NIST recognizes that the US is dependent on commercial products developed and built globally and works cooperatively with international partners. NIST then works with other countries governments in describing the NIST Risk Management Framework, the lessons learned from its development and shares the guidance with other governments. NIST works directly with many governments on incorporating the NIST body of work into their requirements which allows industry and commercial products a similar set of cybersecurity descriptions and outcomes used for multiple, international partners.

<u>Future priorities and recommendations:</u>

New Globally Acceptable Cryptographic Technologies
NIST continues to work with other countries, in standards bodies and with industry on new cryptographic technologies to address the information challenges of the future. These include quantum resistant cryptography, pairing based cryptography, homomorphic encryption and new lightweight cryptographic capabilities.

Use of Machine Learning and Artificial Intelligence in Cybersecurity
NIST conducts research and development is the use of AI/ML for security capabilities in automation of security incident identification and response activities to measurably increase accuracy and time to respond for security incidents. NIST also looks to securing AI/ML systems as part of this program to ensure that trust extensions to AI/ML results in positive outcomes and improved security.

Securing New Forms of High Performance Computing Platforms
In July of 2015, the President issued Executive Order 13702 to create a National Strategic Computing Initiative (NSCI). The goal of the NSCI is to maximize the benefits of High-Performance Computing (HPC) for economic competitiveness and scientific discovery. Security for HPC systems is essential for HPC systems to provide the anticipated benefits. NIST is conducting research to identify security priorities and principles that should be incorporated into the strategy of the NSCI and to identify and prioritize gaps for security that should be addressed.

Addressing cybersecurity standards in governmental multi-lateral organizations
There has been an increased focus on cybersecurity standards in multi-lateral organizations such as the ITU, G-20, G-7, and the OECD. Some governments are seeking to gain buy-in and endorsement for approaches that could enable a greater government role in picking certain technologies, and potentially weaken the important role that the private sector plays in the development and deployment of standards. The net effect of some of these positions could be to weaken the efficacy of cybersecurity standards or result in the cybersecurity standards being used for protectionist purposes. The U.S. government could leverage the IICSWG to shape US government proposals (pro-active) and responses (reactive) to cybersecurity standards related proposals being considered within these organizations.

IoT cybersecurity standards
With the proliferation of IoT applications and growing complexity and interconnectedness of devices, there is a pressing need for standards that will enable greater confidence in product functionality, interoperability, data exchange, communication, etc. Despite this, limited resources and availability of expertise has created tension around what standards to develop first and where to develop those standards.

Priority III - Advocating for U.S. Cybersecurity Products and Services Internationally

Digital Trade Officers and Intellectual Property Attachés

In addition to its Foreign Commercial Officers, the Department has a network of digital attaches located in strategic markets tasked with helping cybersecurity exporters, along with other digital exporters, gain market access and navigate foreign digital policy and regulatory issues.[9] In addition, USPTO Intellectual Property Attachés aid U.S. embassies, consulates, and international missions.[10] The attachés advocate improving intellectual property policies, laws and regulations abroad, work to combat software piracy, and provide information to help U.S. stakeholders entering foreign markets or conducting business overseas.

Cybersecurity Trade Missions

Recognizing the existing global opportunities for U.S. cybersecurity technologies, the Department of Commerce led cybersecurity trade missions to Poland and Romania in 2015 and Japan, South Korea and Taiwan in 2016.[11] The Department of Commerce will also lead a trade mission to Canada in September 2017. Trade missions provide a commercial platform for U.S. companies that want to sell their services and products abroad, gain market intelligence or establish relevant business relationships in foreign markets.

EU-U.S. and Swiss-U.S. Privacy Shield Frameworks

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks[12] are mechanisms designed to comply with data protection requirements when transferring personal data from the European Union or Switzerland to the United States. U.S. companies certified under these frameworks must take reasonable and appropriate measures to protect personal data from being lost, misused, accessed without authorization, disclosed and being altered or destroyed, among other requirements. Although these frameworks are not cybersecurity-specific, they do enable cybersecurity companies to transfer data across the Atlantic. The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks are directly administered by the Department of Commerce. As of June of 2017, there were 2,200 U.S. companies certified under these frameworks.[13]

APEC Cross Border Privacy Rules

Similarly to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, the APEC Cross Border Privacy Rules[14] provide a platform to transfer personal data between several APEC economies and the United States. Companies certified under the APEC Cross Border Privacy Rules need to implement reasonable security safeguards to protect individuals' information from loss, unauthorized access or disclosure, or other misuses. The Department of Commerce is actively

[9] The Digital Attaché Program - https://www.export.gov/digital-attache

[10] *See* Intellectual Property Attaché Program, U.S. Patent and Trademark Office website, https://www.uspto.gov/learning-and-resources/ip-policy/intellectual-property-rights-ipr-attach-program/intellectual.

[11] http://2016.export.gov/trademissions/cybersecureeurope/

[12] EU-U.S. and Swiss-U.S. Privacy Shield Frameworks - https://www.privacyshield.gov/welcome

[13] EU-U.S. and Swiss-U.S. Privacy Shield Frameworks List - https://www.privacyshield.gov/list

[14] APEC Cross Border Privacy Rules- http://www.cbprs.org/

promoting the APEC Cross Border Privacy Rules by aiming to increase the number of U.S. companies and economies participating in the system.

Trade Policy Advocacy
The Department of Commerce advocates for trade policies advantageous to the U.S. cybersecurity industry. Revisions and comments on foreign cybersecurity laws and regulations, government-to-government engagements and roundtables and trade missions are examples of some of the ways the Department of Commerce advocates for business-friendly regulations that serve to facilitate digital trade.

Future priorities and recommendations

Facilitate International Data Flows
Supporting and facilitating data flows is a current and ongoing priority for the Department of Commerce. According to a report by the McKinsey Global Institute, data flows led to a 10 percent increase in world GDP in 2016.[15] Supporting and fostering the growth and success of the U.S. cybersecurity industry and respecting intellectual property rights will be critical to enable the continuous and incremental volume of upcoming global data flows.

Focus on Inclusion of Cybersecurity Provision in Trade Agreements
Free Trade Agreements provide frameworks that serve to facilitate trade and investment among countries which is one of the core competencies of the Department of Commerce. The Department of Commerce believes that future trade agreements should incorporate substantial content regarding cybersecurity practices that serve to facilitate digital flows and trade.

Expand APEC Cross Border Privacy Rules
With current participation of five countries (United States, Canada, Japan, Mexico and South Korea), the Department is actively promoting the APEC Cross Border Privacy Rules as a viable and effective mechanism to facilitate data flows within the Asia-Pacific region. With that goal in mind, the Department hopes to see more economies joining the APEC Cross Border Privacy Rules in the near future.

International Market Access Advocacy and Combating Trade Barriers
Current and potential trade barriers limit market access for U.S. cybersecurity products and services. Some countries currently impose and/or may potentially impose misguided cybersecurity policies and regulations that could limit the ability of U.S. digital companies to do business abroad. The Department of Commerce utilizes a variety of commercial diplomacy approaches that serve to reduce or eliminate trade barriers detrimental to U.S. exporters and the U.S. economy.

[15] McKinsey Global Institute Report 2016 - http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows

Priority IV

Examples of past and ongoing work

Domain Name Security
The deployment of the DNS Security Extensions (DNSSEC) on the global Domain Name System (DNS) is an example of the Department's multiple roles in improving the security and stability of the Internet. The Domain Name System (DNS) is a global distributed database that maps human readable name (e.g. commerce.gov) to various forms of network information. DNS queries are often the first step in any network communication, but are also susceptible to spoofing. NTIA and NIST worked together to address this issue in an effort to enhance the security and stability of the DNS. This multiyear effort included input from technical experts and the broader global multistakeholder community. NIST researchers were part of the development team that created the DNS Security Extensions (DNSSEC) standards in the Internet Engineering Task Force (IETF) standards development organization. DNSSEC provides authentication and integrity protection for the DNS, and protects users from being redirected by an attacker. In July 2010, DNSSEC was deployed at the authoritative root of the DNS to help protect Internet users against various types of cyberattacks.[16] This effort marked the most significant technical change to the DNS and created a more secure user experience on the Internet.[17]

DNSSEC essentially gives a "tamper proof seal" to the address book of the Internet, and in so doing, gives Internet users greater confidence in their online experience. As a result, Internet users will have greater confidence that when they visit a particular website – whether it be their bank, retailer, or doctor – they are not seeing a spoofed copy that cybercriminals can use to perpetuate identity theft or other crimes using the DNS.

DNSSEC deployment at the authoritative root was an important step toward protecting the integrity of DNS data and mitigating attacks such as cache poisoning, which allows an attacker to redirect traffic to fraudulent sites, and other data modification threats. It was an important milestone in the ongoing effort to increase Internet security and build a safer online environment for users. The deployment of DNSSEC at the root is the linchpin to facilitating its deployment throughout the world and enabling the current domain name system to evolve into a significant new trust infrastructure for the Internet.

As DNSSEC is a type of public key infrastructure (PKI), multiple private and public keys are required to make it work. The Key Signing Key (KSK) of the authoritative root zone DNSSEC implementation will be changed (known as a key roll or rollover) for the first time since being deployed.[18] While from a technical perspective this has been thoroughly planned and tested for, it is imperative that the broader global community, particularly Internet Service Providers and

[16] See NTIA DNSSEC, https://www.ntia.doc.gov/category/dnssec (last visited May 12, 2016).
[17] ICANN, VeriSign, Final Report on DNSSEC Deployment Testing and Evaluation in the Root Zone (May 26, 2010), available at https://www.ntia.doc.gov/files/ntia/publications/dnssec_05282010_0.pdf.
[18] *See* Root Zone KSK Rollover, *available at:* https://www.icann.org/resources/pages/ksk-rollover.

other resolvers who have implemented DNSSEC, be made aware of the impending KSK rollover and take actions to ensure there is no disruption in DNS resolution. NTIA and NIST will work domestically as well as with the broader global community in making sure that necessary outreach and steps are taken leading up to and during the KSK rollover process (scheduled to be completed in August 2018).

Secure Inter-Domain Routing

There are known systemic vulnerabilities in the Internet's global routing system, the Border Gateway Protocol (BGP).[19] These vulnerabilities create serious security problems on the Internet. Such attacks and errors potentially disrupt Internet traffic, divert traffic to malicious sites, enable surveillance and economic espionage, and/or outright traffic loss.

NIST, in collaboration with the DHS Science and Technology Directorate, has been working with the Internet industry to design, standardize and foster deployment of security extensions for BGP.[20] Working within the IETF, technical specifications have been developed for three primary technologies necessary to secure the Internet's global routing infrastructure. (1) A global Resource Public Key Infrastructure (RPKI) to enable third parties to cryptographically validate claims of ownership of Internet address blocks and AS numbers, and to permit such resource holders to declare routing relationships. (2) BGP protocol extensions and tools to allow Internet routers to use RPKI information to detect and filter unauthorized route announcements (Origin Validation). (3) BGP protocol extensions to further leverage the RPKI to enable BGP routers to cryptographically verify the complete sequence of networks that comprise a BGP route (Path Validation).[21] NIST has provided technical leadership in the design, specification, and test and evaluation of these new security extensions. NIST researchers have contributed extensive modeling and analysis, prototype implementations, and development of test and measurement tools to facilitate the development of these specifications and to foster commercial deployment.[22]

IPv6 promotion

Every device that connects to the Internet requires an IP address. However, the tremendous demand for Internet connections has, for all intents and purposes, exhausted the supply of IP addresses available under the legacy Internet Protocol version 4 (IPv4) system.[23] IPv6 is the next-generation protocol which provides an identification and location system for computers on networks, and which routes traffic across the Internet. The transition to IPv6, which was designed to expand the number of IP addresses, is critical for the continued, sustainable growth of the Internet. While IPv4 provides nearly 4.3 billion IP addresses, IPv6 offers 2^{128} (or 340,282,366,920,938,463,463,374,607,431,768,211,456 IP addresses), a number more able to

[19] *See* RFC 4272, BGP Security Vulnerabilities Analysis, *available at:* https://www.ietf.org/rfc/rfc4272.txt.

[20] *See* BGP Security and Routing Robustness, *available at:* https://www-x.antd.nist.gov/BGP_Security/.

[21] *See* Secure Inter-Domain Routing (sidr), *available at:* https://datatracker.ietf.org/wg/sidr/about/.

[22] See: "Robust Inter-Domain Routing Project", available at: https://www.nist.gov/programs-projects/robust-inter-domain-routing

[23] *See* "Remaining IPv4 Addresses to be Redistributed to Regional Internet Registries – Address Redistribution Signals that IPv4 is Nearing Total Exhaustion," May 2014, *available at:* https://www.icann.org/news/announcement-2-2014-05-20-en.

meet the rising demand for Internet connections and to support the expanding Internet of Things. This demand will continue to grow as more devices come online.

Even during the relatively early days of the Internet, its exponential growth soon exposed the limitations of IPv4. Once the Internet technical community realized in the early 1990s that there would be a shortage of IP addresses, the IETF began developing a new protocol to expand the Internet address space. The first specification of the IPv6 standard was published in 1995 and an updated draft followed closely thereafter in 1998.[24] Despite the long history of IPv6, today only 32 percent of the Internet services in the United States are IPv6 capable.[25] While the IPv6 adoption rate in the United States is growing at a quicker pace than in the past, companies and other organizations that have yet to plan for IPv6 should begin implementation now rather than later, in order to lay a solid foundation for the future of our digital economy.

In light of this, NTIA and NIST are actively engaged in IPv6 promotional and other efforts. NTIA held a public workshop on IPv6 in 2010 and in 2011 developed the IPv6 Readiness Tool for Businesses, a comprehensive checklist for businesses preparing to deploy IPv6.[26] NTIA also joined a number of private and public organizations in 2011 for the Internet Society's World IPv6 Day to test the IPv6 functionality of websites and services. In late 2017, NTIA issued a request for comments (RFC) that sought information from enterprises on their experiences in implementing IPv6 to guide NTIA in its international and domestic promotional activities and public policy positions. Following up on the information received as part of its 2017 RFC, NTIA is actively considering future and forward looking promotional activities as well as other potential programs that would positively impact broader adoption and use of IPv6.

The Office of Management and Budget (OMB) tasked NIST in 2010 to develop the technical infrastructure of standards, profiles and testing necessary to support the USG initiatives to procure and deploy IPv6 across the federal government. In response, NIST developed the USGv6 Profile and Testing program that provides the technical basis for IPv6 acquisition and developed security guidance and operational test and measurement systems to assist USG agencies in the secure and robust deployment of IPv6 technology.[27] Today the USG is a world leader in the adoption of IPv6. NIST continues to update and maintain its standards and product testing infrastructure and continues to provide test and measurement services to all federal agencies deploying IPv6.

Cryptographic functions

[24] *See* "Internet Protocol, Version 6 (IPv6) Specification," December 1998, *available at*: https://tools.ietf.org/html/rfc2460.

[25] According to measurements conducted by the Asia Pacific Network Information Center, *available at*: https://stats.labs.apnic.net/ipv6/.

[26] NTIA also coauthored a study with the National Institute for Standards and Technology in 2006, entitled "A Technical and Economic Assessment of IPv6." These and other resources are listed on the "Additional IPv6 Resources" page on NTIA's website, *available at*: http://www.ntia.doc.gov/page/additional-ipv6-resources.

[27] *See* "USGv6: A Technical Infrastructure to Assist IPv6 Adoption," *available at:* https://www-x.antd.nist.gov/usgv6/index.html

NIST is responsible for developing standards (Federal Information Processing Standards, or "FIPS")[28] and guidelines to protect non- national security federal information systems. Cryptographic standards and guidelines for the protection of federal information systems have always been a key component of this effort. They must be robust and have the confidence of the global cryptographic community in order to be widely adopted and effective at securing information systems worldwide. Outside the Federal Government, these publications are voluntarily relied upon across many sectors to promote economic development and protect sensitive personal and corporate information. NIST has a dual role in this regard: 1) as a developer of standards and guidelines under federal law, and 2) as a technical contributor and stakeholder in connection with voluntary, global standards development.

To ensure these standards and guidelines provide high quality, cost-effective security mechanisms, NIST works closely with a broad stakeholder community to identify areas of need and develop standards and guidelines. That community has expanded in recent years and now is global in nature, as is the interest in having systems in place that will appropriately protect and ensure the security of digitized information. That community includes experts from academia, government agencies, and organizations that choose to adopt NIST cryptographic standards and guidelines. Open and transparent processes are critical to developing the most secure and trusted cryptographic standards possible. NIST strives to engage all of its stakeholders in these processes, and continually works to strengthen its efforts in this area.

Perhaps the most notable examples of international cooperation within the cryptographic community are the international block cipher and hash algorithm competitions, which resulted in the Advanced Encryption Standard (AES) and the Standard Hash Algorithm-3 (SHA-3).[29] Among ongoing activities, submissions are currently being accepted by the Post-Quantum Cryptography Standardization Project. These activities have coalesced the international cryptographic community in pursuit of common goals, and promote broad acceptance of Federal cryptographic algorithm standards.

Transport Layer Security

The Transport Layer Security (TLS) protocol is arguably the most important security protocol on today's Internet, providing security for retail e-commerce, banking applications, and other client/server applications that require protection against eavesdropping, tampering, or message forgery. TLS is an IETF standard, and replaced the proprietary Secure Sockets Layer (SSL) protocol, which was designed to establish a secure channel between a web server and a browser. TLS fulfills this function, but is also widely used for machine-to-machine communication to

[28] *See* Federal Information Processing Standards Publications (FIPS PUBS), *available at:* https://www.nist.gov/itl/popular-links/federal-information-processing-standards-fips.

[29]*See "Federal Information Processing Standards Publication 197 Announcing the Advanced Encryption Standard (AES),"* November 2001, *available at:* http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf and *see* SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, August 2015, *available at:* https://www.nist.gov/publications/sha-3-standard-permutation-based-hash-and-extendable-output-functions?pub_id=919061.

secure applications and various administrative functions. TLS has also been extended to support "connection-less" applications in the Datagram TLS (DTLS) standard.

While TLS has been around since 1999, the IETF continues to refine the protocol and improve the security guarantees. TLS Version 1.3 is currently under development, and introduces a number of performance and security enhancements. The National Institute of Standards and Technology (NIST) actively participates in the IETF process to ensure that US government applications can take advantage of these enhancements.   Most significantly, TLSv1.3 only specifies cipher suites that support perfect forward secrecy (PFS.) With PFS, future compromise of key material does not compromise the security of past sessions.) Previous versions of TLS included cipher suites that did not offer this guarantee. NIST works within the IETF to ensure that US government cipher suites can be used with the emerging TLS v1.3 protocol.

Large enterprises currently use TLS v1.1 and v1.2 with cipher suites that do not support PFS to enable troubleshooting, traffic monitoring, and audit compliance. NIST is working with the banking and health care communities to develop secure and scalable mechanisms to support troubleshooting, traffic monitoring, and audit compliance within enterprise datacenters using TLS v1.3 in a standards compliant manner. This work will be performed at the National Cybersecurity Center of Excellence and coordinated with the IETF.

Software Defined and Virtual Networks

In response to dramatic changes brought by virtualized computing, industry has developed new initiatives in Network Function Virtualization (NFV) and Software Defined Networking (SDN). These are radical departures from today's industry norms, in that they abstract the implementation of new network functions and decouple them from specific hardware platforms and topological constraints (i.e., the location in a network where functions/services must be deployed). In essence, NFV/SDN make the network itself "programmable," offering the promise of rapid innovation of network services customized and tightly integrated with specific application domains. NFV/SDN will enable the networking industry to follow the same virtualization model that cloud computing has successfully demonstrated with both cost savings and business growth measured in the billions of dollars. The results of NFV/SDN research and development are creating fundamentally new measurement challenges in network behavior, software quality, and security properties of dynamically composed, programmable networks.

Given the critical position of basic network control systems, the need to accurately measure and thoroughly test the safety, robustness, security and performance of software defined networks will be paramount in ensuring the success of these technologies use in future mission/business-critical networks. NIST is working to develop test and measurement techniques to advance the state of the art in network virtualization, network service function chaining, software defined networks, technologies and techniques to address robustness safety and security of virtualized network services. In the future, the Department aims to explore novel applications of NFV/SDN to domains such as network security and intrusion detection, support of machine-to-machine communications, support of advanced mobility and cloud computing.

Improved Cryptography for Internet Communication
The Internet is increasingly relied on as a vital part of business processes. Sometimes these processes involve the transmission of sensitive information. This means that public and private enterprises need to protect the confidentiality of Internet communication. There are protocols to protect Internet communication, but as computing power increases, and new protocols are developed, these security protocols need to be revised. The Department continues to work on improving the security of Internet communication. Agencies participate in various Internet standards bodies to develop new, and improve current secure network protocols for Internet communication. This also includes the development and refinement of new cryptographic algorithms for use in protecting communications. NIST works with academia and industry in holding workshops and contests to develop the next generation of cryptographic algorithms. These algorithms are then added to network protocols to provide improved security in communication.

Priority V

<u>Examples of past and ongoing work</u>

United States Telecommunications Training Institute (USTTI)
One example of the Department's internationally-focused cybersecurity and ICT education is NTIA's capacity building programs conducted in partnership with the United States Telecommunications Training Institute (USTTI). USTTI is a non-profit public-private partnership with over 32 years of experience providing tuition-free telecommunications and ICT training for entrepreneurs and government officials from developing countries. Since 2004, NTIA has provided annual USTTI training courses on ICT policy-making, cybersecurity and multistakeholder decision-making. More than 500 developing country participants from government and the private sector have attended these NTIA programs.[30]

The National Initiative for Cybersecurity Education (NICE)
NIST's National Initiative for Cybersecurity Education (NICE) is a partnership between government, academia, and the private sector that seeks to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with public and private sector partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our Nation secure. The NICE Strategic Plan includes the objective to collaborate internationally to share best practices in cybersecurity career development and workforce planning.[31]

[30] http://ustti.org/news/index.php?UpdateID=134
[31] https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan

NICE Cybersecurity Workforce Framework (NICE Framework)

The NICE Cybersecurity Workforce Framework (NICE Framework) serves as a fundamental reference resource to support a workforce capable of meeting an organization's cybersecurity needs. It provides organizations with a common, consistent lexicon that categorizes and describes cybersecurity work. Using the NICE Framework as a reference resource will improve the communication needed to identify, recruit, and develop cyber- security talent. Learn more at www.nist.gov/nice/framework.

USPTO Global Intellectual Property Academy (GIPA)

The USPTO's Global Intellectual Property Academy (GIPA) offers programs on a full range of intellectual property topics including the protection of patents, trade secrets, trademarks, and copyright.[32] The programs are offered in the United States, abroad, and over the Internet through webcasts and e-learning initiatives in several languages. Training for foreign government officials and for U.S. small to medium sized enterprises is a high priority for GIPA. Over the last ten years, GIPA training programs have increasingly focused on intellectual property issues in the digital economy.

The USPTO has also been actively involved in efforts to foster voluntarily developed codes of conduct for improving online enforcement. In particular, the Office of the U.S. Intellectual Property Enforcement Coordinator's 2013 Joint Strategic Plan for Intellectual Property Enforcement provided that "[a]s part of the effort to determine whether voluntary initiatives have had a positive impact on reducing infringement, USPTO will solicit input from the public and other parts of the U.S. Government and will initiate a process to assess the effectiveness of voluntary initiatives."[33] USPTO has received input and is currently considering strategies for evaluating the effectiveness of voluntary initiatives

<u>Future priorities and recommendations</u>

International NICE priorities

The National Initiative for Cybersecurity Education (NICE) plans to convene the partners of the Five Eyes (Australia, Canada, New Zealand, and the United Kingdom) and other key international partners at the RSA Conference in 2018 to explore opportunities for collaboration and partnership on cybersecurity education, training, and workforce development. One possible outcome of the initial convening is an International Summit on Cybersecurity Education and Workforce or a series of international meetings among government, academia, and industry.

[32] USPTO Global Intellectual Property Academy, http://www.uspto.gov/learning-and-resources/global-intellectual-property-academy (last visited May 13, 2016).

[33] U.S. Intellectual Property Enforcement Coordinator, 2013 Joint Strategic Plan on Intellectual Property Enforcement (June 2013), available at https://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf.

The National Initiative for Cybersecurity Education (NICE) would also like to explore the adoption of the NICE Cybersecurity Workforce Framework as an internationally recognized standard for use by education and training providers who develop educational programs and curriculum, as well as employers who seek to recruit, hire, develop, and retain a cybersecurity workforce.