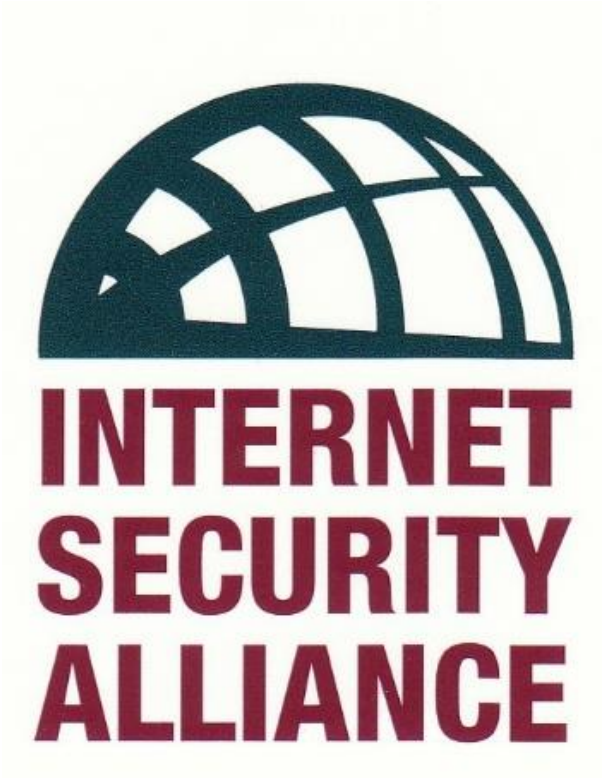
Input to the Commission on Enhancing National Cybersecurity



2500 Wilson Blvd. Suite 245
Arlington, VA 22201

The Commission seeks information on the following topics:

Critical Infrastructure Cybersecurity

Executive Summary

Topics Addressed

This section of our comments addresses issues faced by eight critical infrastructure sectors. The authors of these comments are mostly chief information security officers for large companies within those sectors. Namely (and in order): Defense Industrial Base; Healthcare; Financial Services; Energy (specifically, local utilities); Information Technology; Telecommunications; Manufacturing; and, Food and Agriculture.

Readers will encounter material about current and future trends; progress being made; the most promising approaches to addressing the challenges; what should be done now or within the next 1-2 years to better address the challenges; what should be done over the next decade to better address the challenges; and future challenges that may arise and recommended actions that individuals, organizations and government can take to best position themselves today to meet those challenges.

Challenges

Because each sector is unique, sector-specific companies face unique sets of challenges. However, some challenges are common among them all. Most notably is the fact that cybersecurity is poised to deteriorate even further in the near future. The attack community is persistent and innovative. Attacks once dubbed an "advanced persistent threat" for their associated danger are now the norm. This situation persists because economic incentives in cybersecurity favor the attackers. Cyberattacks are cheap and profitable, while the private sector faces systemic disadvantages in defense, including competitive pressure to adopt new technologies and businesses practices that undermine good security.

Recommendations

While each sector is unique, there's agreement across sectors that policy makers must address the economic imbalance fueling poor cybersecurity. Proponents of cybersecurity regulations typically do not address the economic impacts of their proposals. They also tend to fail to explain exactly how a regulatory regime would operate effectively. For example, the health care sector has long been regulated for cybersecurity and it has one of the worst security records of any sector. Further, regulatory proponents fail to describe how such a system can be managed without inhibiting innovation, economic growth and international competitiveness. For industries where regulation is an inherent part of their economics (e.g. municipal water utilities), regulation can be used, but for the vast majority of the economy, regulation will be ineffective and counterproductive. Regulations necessarily lag the appearance of new attack methods and create a burden of compliance costs that siphon money from actual cybersecurity—as well as fostering a compliance mentality antithetical to good security.

An incentive program as contemplated in the House GOP Task Force Report on Cybersecurity and President Barack Obama's Executive Order 13636 which has not been fully implemented, will provide a vastly more dynamic, flexible and effective way to promote continued cybersecurity. Incentives need not be tax breaks. Multiple alternatives including streamlining audit requirements, fast tracking permits or patents or regulatory forbearance for good actors stimulating private insurance, liability benefits and other models described herein should be tested and implemented. Carrots that address the economic roots of our cyber problem rather than regulatory sticks focused on the technical methods of cyberattacks will make the nation's critical infrastructure more secure.

Cybersecurity in the Defense Industrial Base (DIB)

What Makes the DIB Sector Unique

The defense industry has a different economic model than most industries, and investing in cyber protection is not a function of traditional economic risk management. Top-tier defense companies sell to national governments with few alternatives, and the Pentagon is unlikely to opt for lower cost products from rival nations, especially should the design suspiciously resemble American-made technology.

The defense industry invests in cybersecurity, despite the lack of traditional economic interest, out of a fundamentally patriotic sense of responsibility to our warfighters and because strong data and network security are essential to brand credibility when doing business with the military.

However, small- and medium-sized companies lower in the defense supply chain have a greater proportion of commercial business than defense business. The greater the commercial component of a business, the more the traditional economic risk-assessment calculations predominate. Financial conditions facing SMBs do not afford them the luxury of uneconomic investments in cybersecurity.

Differences in incentive structures have created a two-tiered defense ecosystem. One tier contains the large, well-funded system integrators and the other everyone else. Into this mix, DoD has introduced new compliance requirements, in an attempt to artificially influence traditional economic-based risk-management calculations.

Challenges Facing the New Administration

Modern weapons systems are built via a supply chain hundreds of companies long, spanning multiple countries and subject to cyber manipulation. Defense developers and innovators are at risk of intellectual property theft through cyber espionage. Second-level nations skip generations of research

development, becoming competitive with US weaponry, and the economic losses portend negative downstream effects on future investment and innovation.

Government reporting and information-sharing requirements are confusing and divert resources away from security to compliance. New regulations have significantly increased costs of doing business with the government and shifted cybersecurity focus from incentives, as called for in Executive Order 13636, to compliance with standards. These increased costs dwarf information technology budgets for small businesses. However, compliance alone will not generate security and must not be confused with it.

The collaboration process codified in the Defense Industrial Base Framework Agreement has been successful but is labor-intensive. Cyber threats have expanded to attack the defense supply chain, an ecosystem of smaller, less cyber-capable companies, ill-suited for such processes.

Cybersecurity policies assume US-based companies operating on American soil. Yet, reductions in defense spending led many companies to expand their presence overseas, creating a very different set of dynamics for cyber defense in the sector. The requirements levied by the International Trafficking in Arms Regulations drives the defense industry into maintaining two distinct networks—one for US persons and one for non-US employees—making a unified cyber defense both difficult and expensive. Privacy laws of many countries also make a unified monitoring environment difficult.

Most countries now require coproduction or offset suppliers. As the demand for coproduction rises in the value chain, so does the need to defend the networks of suppliers, resulting in policy challenges to the defense industry in two areas: first, current information-sharing policies preclude open sharing of information with foreign partners; second, the Defense Federal Acquisition Regulation Supplement rules on safeguarding defense information mandate application of NIST controls to overseas suppliers anytime covered information is involved. But few foreign companies are likely to submit themselves to DoD-imposed standards, leaving defense companies to choose between continuing with a foreign

supplier who is out of compliance or abandoning the supplier and failing to meet contractual offset requirements.

Recommendations

Institute a Tiered Model for Grading Cybersecurity Competency

The current regulatory compliance model is binary—either comply with everything or fail. Turn it into an incentive model with different tiers of compliance, where each level represents a concrete improvement in security. Companies will then prioritize efforts, and the government and larger defense contractors could tailor contract requirements to a certain level of security, incentivizing suppliers to move to the next tier to gain eligibility for larger contracts. This would transform the compliance environment to a competitive one, which will then incentivize defense companies to advance tiers in order to set themselves apart from their peers or gain market share. A maturity model would also allow small- and medium-sized defense contractors to realistically participate.

Information Sharing beyond the Elites

Current close-hold information-sharing methods are designed for companies with the infrastructure and staff capable of manually receiving complex threat data, evaluating these data for their environment, and applying them to any number of defensive systems. Small companies cannot do this. Instead, sharing with small companies requires a passive model where the company can accept threat data in an automated system and have these data applied to their network. The Pentagon needs to work with industry to create a broader information-sharing environment that is affordable and passive. Defense can allow large system integrators to share DoD-provided, unclassified threat indicators with defense contractors in their supply chain via automated monitoring systems. Extending to the supply chain can have a high payoff at a low cost.

DoD Should Move to Better Accommodate a Global Defense Industrial Base

Defense needs to work with industry to develop operating concepts for cyber defense in an increasingly global market. Compliance regimes and information-sharing processes must both be modified to accommodate overseas suppliers and coproduction agreements. They must also work to develop a way to share cyber-defense information with foreign suppliers of critical items. DoD should work with NIST to find an acceptable international standard that can serve as an overseas substitute for defense-controlled-information cybersecurity controls.

The Pentagon Needs to Increase Its Focus on Small Businesses

Defense depends on small businesses to support its missions, spark innovation, and develop technologies to support soldiers. While the Office of Small Business Programs has acknowledged that cybersecurity is an important and timely issue for small businesses, it has not identified or disseminated any cybersecurity resources in its outreach and education efforts to defense-sector small businesses. The next administration should ensure cybersecurity is a part of the OSBP outreach and take steps to stabilize the office's performance and leadership team.

Cybersecurity in the Healthcare Industry

What Makes the Healthcare Sector Unique

Patient data are uniquely valuable to criminals. The cost of purchasing stolen patient records on the cyber black market is approximately ten times the cost of purchasing that same individual's stolen credit-card data and includes all data elements necessary to impersonate the victim. Hackers further monetize health records by compromising weaknesses in the health-care system, billing fraudulent claims to Medicaid and Medicare, potentially prescribing narcotics, and even filing fraudulent tax returns.

Perhaps the most interesting evolution in the cyber threat facing health-care industry is the rise of the nation-state threat. Governments of other countries direct their cyber warriors to hack into hospitals and health insurers to steal medical records. It's likely that nation-state actors are stealing patient data to build databases on American citizens for espionage activities.

Insider threats are particularly insidious in the healthcare sector. Healthcare data processors say malicious insiders account for just about 10 percent of data breaches but are the root cause of double the percentage of medical-identity thefts. Accidental insiders cause more, albeit smaller, breaches.

The number of individuals who have access to data during a healthcare transaction represents another point of vulnerability. Even a routine visit to the doctor exposes medical data to a dozen people or organizations as diagnostic and billing information makes its way through various systems. Each hand represents another potential point of vulnerability or attack.

Challenges Facing the New Administration

Two major laws governing healthcare cybersecurity practices are not functioning as intended. The massive 2013 omnibus rule updating HIPAA, mandated by the HITECH Act, has failed to have the desired

effect of making the healthcare industry more secure. In the years since its implementation, massive health-payer data breaches have occurred.

Moreover, the regulations take a retributive approach to cybersecurity, punishing organizations that get breached. Breaches spawn regulatory actions that often lead to punitive outcomes in the form of substantial fines and other penalties, regardless of how much time and money was put into trying to prevent a breach.

The cost of security is a great obstacle for healthcare organizations. Large organizations have the ability to fund teams dedicated to both implementation of security best practices and regulatory compliance. Small practices have minimal resources. While all organizations must abide by the same rules and regulations, not all have equivalent access to the financial resources and expertise necessary to comply. The high cost of compliance, and the higher cost of failure, further exacerbates the problem.

The doctor-patient relationship is unique—patients are unlikely to abandon their medical provider over a data breach, so there is little incentive beyond regulatory consequences to spend time and effort defending against potential breaches.

The proliferation of technology in healthcare is another obstacle. Like most disruptive technologies, the uses for mobile-enabled practice management systems multiplied long before any serious thought was given to securing the technology.

Escalating ransomware attacks on the healthcare industry creates another challenge. For now, ransomware attacks appear unconnected to data theft. But given the real value of patient data—in its theft for exploitation or resale—ransomware attacks will become the nasty second jab of what really are one-two punch attacks.

Possible cyber-terrorist attacks against newly networked medical devices coming onto the market could cause significant disruptions, some even fatal. Life-sustaining devices once isolated away from public networks are now exposed to them. Medical equipment is now part of the mix of databases and hard drives once thought impervious to hackers.

There's also a lack of urgency within the healthcare industry. The idea that medical data had value to criminals is novel, and it took significant healthcare data breaches to convince the industry to get serious about committing resources to secure itself against cyberattacks.

Recommendations

Incentivize Healthcare to Implement Best Cybersecurity Practices

Healthcare needs a shift in focus away from prescriptive regulation toward regulation that encourages security best practices. An incentive-focused regulatory approach would encourage more healthcare companies to invest in necessary protections to information assets, possibly even driving broad adoption of controls necessary to solve the aforementioned data problems. What's needed is a sliding scale of liability protection on the basis of company's progress toward implementing an objective set of practices. The NIST Cybersecurity Framework, and the process used to develop it, could provide a good starting point for determining those practices.

The system should allow a company to accrue credits tied to its investments in security that it could use against future regulatory action and fines in the event of a breach. This could be taken further by also offering modest tax incentives for certain high-value, but often-overlooked, security best practices, such as employee awareness training.

Reduce Regulatory Complexity

Congress should pursue legislation that harmonizes privacy, security, and information-risk-management requirements to eliminate the complex patchwork of regulations. Streamlining HIPAA audit requirements put into place by the HITECH Act. These types of compliance audits drain resources from security budgets. Adequately complying with regulatory requirements, combined with proof of ongoing investment into cybersecurity, should result in a less strenuous oversight the next time around—a HIPAA-Lite version, as it were—or increased time interval between compliance audits.

Replace Social Security Numbers as a Patient Identifier

Congress should remove language placed annually in federal spending bills that prohibits the Department of Health and Human Services from using any federal funds to promulgate or adopt any such standard. Technology has provided for alternatives to a numeric or alphanumeric identifier as a solution, and the government does not need to be the arbiter of the identification solution.

Use Security as a Factor of Reimbursement

Congress should allow the Centers for Medicare and Medicaid to use security as a factor in reimbursement. Similarly, improving an organization's cybersecurity readiness should be considered a recognized activity under the clinical practice improvement performance category under the Medicare Access and CHIP Reauthorization Act Merit-based Incentive Payment System reimbursement scheme.

Cybersecurity in the Banking and Financial Sector

What Makes the Financial Services Sector Unique

Banks and other financial institutions remain a top target for cyberattacks, whether for financial gain, data theft, or retaliation. Today's consumers have higher expectations about service, given the proliferation of technologies available to them. Consumers are more likely to shop around for products and be more interested in direct and mobile channels. However, while the use of innovations such as mobile devices and applications for consumer banking has exploded, the exploitation of these devices has increased significantly.

Commercial banking, too, has seen tremendous benefits from technology and is poised to reap even more as the new distributed ledger system, known as blockchain, enters the mainstream. More than half of exchanges surveyed by the International Organization of Securities Commissions and the World Federation of Exchanges in 2013 reported experiencing a cyberattack during the previous twelve months. Neither is the insurance industry immune to the changes in how business is conducted in today's contemporary and interconnected society. Insurers are prime targets to be victimized, given the richness of data—credit-card information, medical information, and other underwriting information.

Challenges Facing the New Administration

The current regulatory model for cybersecurity does not work. Cyber technology and attack methods change constantly, and the regulatory process is inherently time consuming and cumbersome.

The financial services sector continues to see an increase in disparate and fragmented cybersecurity regulation. For many institutions, it began with the Federal Financial Institutions Examination Council releasing in June 2015 a Cybersecurity Assessment Tool incorporating concepts from the voluntary NIST Cybersecurity Framework. Member agencies use the tool in regulatory inquiries. As a result, many large

financial institutions expend immense amounts of time and resources determining how to demonstrate compliance.

Complicating matters further, financial institutions receive similar cybersecurity inquiries from different regulators, even from different offices of the same regulator. These duplicative reporting requirements ask largely the same questions but require exhaustive tailoring for each regulator. And the SEC is becoming ever more assertive in monitoring the cybersecurity of broker-dealers and registered investment advisers.

Technology innovations have eliminated borders for criminal enterprises. Attackers can exploit vulnerabilities from anywhere and impact entire networks in a matter of seconds. This poses a tremendous risk of cascading failure across the sector. Phishing is a main pathway for cyber theft, and spear-phishing is even more pernicious. The use of phishing is widespread, unrelenting, and a low-cost, high-payoff technique for attackers.

Mobile banking is a boon for consumers but opens up a new front for attackers to exploit. Cyber thieves craft malicious apps targeting banking data, but it's not just banking apps that pose a cybersecurity challenge.

Recommendations

Government Should Rethink Its Approach to Cybersecurity

The federal government's credibility in educating, let alone regulating and mandating, cybersecurity practices is severely undermined by its track record of inefficiency. Agencies have yet to adjust to the interconnected nature of cybersecurity, approach it as if it were a static problem addressable through existing formulations. Punitive checklist compliance is a waste of resources. The number of regulatory agency examiners with specialized information technology training is low, and much of government's shared cyber-threat data are out of date and stripped of context as to be useless.

Harmonize, Streamline, and Improve Regulations

Regulatory and legislative mandates and compliance frameworks that address information security for the financial sector, such as Sarbanes-Oxley, Gramm-Leach-Bliley, the Fair and Accurate Credit Transactions Act, as well as state compliance regimes, must be consolidated and streamlined.

Regulations should encourage banks to take a risk-based approach, which is customized to the threats they face and takes into account the bank's business model and resources available. Utilizing a standard mechanism such as the NIST Cybersecurity Framework to align the proliferation of different legal and regulatory cybersecurity requirements enables harmonization and adopts unified fundamental guidance for developing cybersecurity policies and practices within the industry.

Operational Improvements

Toss the Password into the Dustbin of History

"Killing the password" has been a long-standing Obama administration priority, one that it reiterated in the National Cyber Action Plan unveiled in February 2016. The new administration should accelerate the work of the National Strategy for Trusted Identities in Cyberspace, a program charged in 2011 with creating market conditions favorable to a wholesale replacement of passwords. Today, it's clear the effort has stalled.

Incentivize ISPs to Become More Active in Cybersecurity

ISPs are critical players in improving cybersecurity across the Internet but are not incentivized to implement well-established security protocols, such as DNS Security Extension and BGPSec, that would make launching cyberattacks harder for hackers. We are not advocating for heavy-handed regulation but a common set of strong security standards that ISPs can be evaluated against in the market place, much like the "5-star safety rating" system developed years ago by the National Highway Traffic Safety Administration.

Adopt Antiphishing Technology

The existing Internet technology standard known as DMARC (domain-based message authentication, reporting, and conformance) should be implemented by the federal government and even further in the private sector.

Encourage Development of More Cybersecurity Experts

The new administration should consider leveraging the federal science, technology, engineering, and mathematics program to promote wider interest among students in technology jobs. The current national goal of graduating an additional one million students with STEM majors should be reassessed with an eye toward increasing both that number as well as the number of technology graduates represented within it.

Cybersecurity in the Power Utility Sector

What Makes the Utilities Sector Unique

Over the past decade, the bulk power system has seen improvements and increased investment in resiliency and cybersecurity. However, local power-distribution assets are not only more vulnerable to cyberattack but also more critical to national electricity delivery than previously contemplated.

Marketplace Innovation Is Lagging

While products to protect information technology infrastructure are readily available and mature, there are far fewer products in the marketplace that provide security for the highly connected operational technologies that control physical assets on the power grid.

To add complexity, many power utility executives struggle with the uncertainties associated with recovery of security-related costs and overhead on the basis of traditional state rate making procedures. Even if there were adequate funding by utilities to address their normal (i.e., “commercial”) cybersecurity risk, there will inevitably be a gap between vulnerabilities that can be cost-effectively mitigated and the residual risk posed by sophisticated nation-state powers seeking to disrupt the grid. Even utilities, duty-bound by public-good considerations, are still private-sector businesses that are unlikely to invest far beyond the thresholds of normal commercial risk.

Limited Information to Inform Cybersecurity Decisions

Exacerbating the situation is how utility asset vendors sell closed-source devices and software solutions, which typically come bundled with significant contractual prohibitions against tampering or reverse engineering. This results in a difficult situation, preventing utilities from processes that might allow them to verify the integrity of hardware and software they purchase.

Challenges Facing the New Administration

A Grid That Is Becoming Increasingly Difficult and Costly to Defend

For the past fifteen years, the electric power industry, with significant support from government, has invested heavily in making the distribution system smarter, more efficient, and more connected. Smart grid technologies have been incentivized and implemented with little regard for the increased cyber risk. Equally concerning is that utilities are sourcing advanced technologies and products from multiple vendors with little or no ability to properly assess supply-chain risks.

Creeping Possibility of a Terrorist Attack

The possibility of terrorist attacks will grow. The level of sophistication required to effect widespread damage to the grid has typically suggested that only nation-states will be effective. However, a growing community of postnational actors are being contracted by states as an extension of their offensive capabilities, which is creating an international marketplace for sophisticated disruption capabilities.

Recommendations

Enhance Information Sharing between Utilities and the Federal Government

Greater federal government transparency in managing data will foster trust and confidence in relationship building and communication. The next president should instruct the existing utility industry sector coordinating council and the corresponding government coordinating council established under the National Infrastructure Protection Plan to engage on these information-sharing issues and report back to the administration within three months on their plan to create greater clarity and transparency regarding information sharing within the sector, including any legislative adjustments that may be needed.

Reform the Clearance Attainment Process for Private Sector Executives

Long processing times and an insufficient number of security clearances being made available are significantly hindering the utility industry's ability to support the US cybersecurity mission. The next

president should instruct DHS to coordinate among security clearance granting agencies and develop an expedited “TSA precheck” style system to enable already cleared individuals to maintain their clearances more easily and generally modernize the clearance process to include the use of transferable clearances from department to department.

Ensure DOE Remains the Primary Liaison between Utilities and the Federal Government

While DHS plays a critical role as utilities face cybersecurity challenges, the Department of Energy remains best suited as the main point of contact due to decades of working to provide meaningful, contextual, and actionable analysis. The next president and Congress should consider amending the Cybersecurity Act of 2015 to expand the benefits currently granted for sharing information with DHS to other appropriate agencies such as Energy.

Catalyze and Accelerate the Development of the Private Cybersecurity Insurance Market

Cybersecurity insurance is an undervalued tool and critical to the future safeguarding of utilities, but to date the market has focused on data-breach fallout. To expand coverage, the administration and Congress should replicate the success of the Terrorism Risk Insurance Act to create a similar reinsurance backstop for cyberattack-caused real-world damage to utilities and their customers.

Promote Innovation through Government Grants

Initiatives such as Rapid Attack Detection, Isolation and Characterization Systems at DARPA and Cybersecurity for Energy Delivery Systems at Energy encourage investment in commercial products by appropriately reducing risk for potential vendors and helping bring together all relevant stakeholders. These programs should be continued and expanded.

Increase Cybersecurity Focus of State-Level Regulators and Legislatures

The federal government should pass a cybersecurity “states-must-consider” law so that states must demonstrate they have considered appropriate cost-effective cybersecurity standards for their electric

utility ratemaking proceedings. Doing so will effectively increase the focus on distribution cybersecurity at the state level without imposing new regulations on distribution utilities.

Encourage Public-Private Collaboration to Manage Vendor Risks

Vendors must play their part in the security of the grid. A new balance needs to be struck between the commercial needs of vendors, who would prefer not to reveal the workings of their products, and the needs of electric utilities to both ensure assets are not prepackaged with malware and understand better how assets would behave if they were to be controlled maliciously. Solving this requires a dialogue between utilities, vendors, and the government to evaluate possible solutions that cost-effectively increase confidence in US grid assets and help utilities prepare for cyberattacks. The Obama administration's proposal for a National Center for Cybersecurity Resilience, where companies could test the security of systems under controlled conditions, is a good start in this direction. So is the Federal Energy Regulatory Commission's proposed rule regarding supply-chain risk management. The government and utilities themselves could play a valuable role in incentivizing vendors to adopt the Underwriter's Laboratories model—this would ensure that all vendor products are rigorously and transparently inspected to ensure they meet baseline cybersecurity standards.

Cybersecurity and the Information Technology Industry

What Makes the IT Sector Unique

In the digital age, virtually all sectors rely on the IT sector, and no industry has escaped transformation because of IT innovations. The Internet changed virtually every aspect of modern life. Approximately 12 percent of global trade is conducted via international e-commerce. Even the political process has changed because of social-media interactions.

Computing power doubles every two years, and interconnected devices communicate and deliver instructions and intelligence to machinery, creating the Internet of Things and amassing huge amounts of data. However, this increase in surface creates ample opportunities for security breaches and the misuse of privacy information that will be felt by all sectors, not just IT.

These same innovations also create ample opportunities for advances in cybersecurity technologies. Development of products with artificial intelligence and the use of machine learning gives us the ability to prevent, predict, detect, and respond to attacks as never before.

However, do not mistake improved technical abilities for a true solution to the bad state of computer security. The challenges are imbedded in policy and management. The IT industry has flourished in a generally unregulated environment, which has been essential to its historic growth and productivity. An unhappy by-product of this growth is a system prone to outside attacks. The sector must find a mechanism to sustainably secure it without killing innovation.

Challenges Facing the New Administration

Internet of Things: In the IoT, humans are the ultimate thing and will generate multitudes of personal data. We know better than to create this world without securing it first, yet we continue to do so.

Cyber war and terrorism: Even absent direct escalation into a shooting war, cyberattacks will cross the plane from bits to atoms and become kinetic in the damage they cause.

Commercial espionage: Intellectual property theft is an act of economic war and harms drivers of global economic growth.

Proposals for backdoors: Adoption of proposals to build encryption backdoors into IT products for law-enforcement and intelligence communities would benefit adversaries, provoke legitimate privacy concerns among citizens, and further deteriorate trust between the United States and world community.

Government cybersecurity: Government systems repeatedly fail at security. Federal information technology infrastructure is obsolete, yet government continues to spend resources on legacy systems rather than funding upgrades.

Information sharing: We cannot seem to navigate the legitimate concerns of privacy groups around information that can be shared and the business community around legal liability. Moreover, liability protections are available only for sharing through DHS and no other preferred entities such as the FBI.

Public-private partnership: Trust and cooperation between IT and government is at an all-time low. This will persist so long as government continues to threaten industry.

Data-breach notification: Forty-seven states plus the District of Columbia maintain separate laws for data-breach notification, creating an undue burden on industry and increasing costs for notification of breaches.

Recommendations

Create a Cabinet-Like Position to Upgrade Civilian IT and Security Infrastructure

Given the importance of IT in the running of our government, the need to manage and secure critical infrastructure, and the ongoing productivity benefits of continued innovation, appointing a cabinet-level position to manage an IT transformation should be one of the highest priorities for the next administration. The position needs full authority and funding.

Workforce Development

Government should work with colleges and universities across the country to obtain a steady flow of recruits for cybersecurity positions by providing scholarships to students willing to commit a specified number of years in government cybersecurity positions.

Increase and Improve International Law Enforcement and Cooperation to Prevent Cyber War and Terrorism

This should start with the president instituting a full review of national law-enforcement spending to assure that fighting digital crime is far better resourced. The commander-in-chief should also initiate a concerted process to modernize international law and procedures with respect to clarifying criminal laws internationally.

Increase Government Research and Development Funding for Risky Technology Research

Rather than routinely cut research and development funding, the United States should emulate what our competitors are doing in other countries by providing increased government support for basic IT research and general-purpose digital programs.

Public-Private Partnership

Collaboration between the public and private sectors to test the effectiveness of the NIST Cybersecurity Framework is needed to define what using the framework entails. By testing the framework, cost-

effective aspects will be discovered. Cooperation would also allow the Enduring Security Framework to be reenergized and expanded to include allies.

Law Enforcement Should Stop Pushing the "Going Dark" Narrative

New enabling capabilities for the IoT and advancements in computer power and storage capacity for big-data applications can be used by law-enforcement, defense, and intelligence communities in lawful ways. Law enforcement should spend more energy in adjusting their investigative techniques to this new world than fighting the inevitable onset of encryption, which is good for cybersecurity by preventing data theft and cyber espionage.

Cybersecurity in Telecommunications

What Makes the Telecommunications Sector Unique

The global telecommunications sector is a mix of government, former government, and commercial operators. The networks are a critical part of the business infrastructure and increasingly seen as part of the critical national infrastructure. They deliver services for customers but also wider benefits for society.

The telecommunications industry stores, manages, and transports a vast amount of valuable data for individuals and society, digital commerce, and critical national infrastructure.

The threat from cyber actors is increasing in sophistication, persistence, and variety—and the risks posed are not easily mitigated. Cybersecurity needs to be multidimensional, transcending the risk management and response capabilities of any single enterprise, industry, or government. The damage inflicted by successful cyberattacks is not just financial and commercial but can also lead to long-term reputational damage and regulatory action.

Customer confidence is crucial. Customers need to know that their data are safe and to understand how companies will use these data and the basis on which the government can secure access to these data. Customers need to trust service providers to behave responsibly in this regard. Telecommunications is a regulated business. Service providers are required to give government's access to customer traffic and data in accordance with licensing regulations and the laws of the jurisdictions in which they operate. Our policy is clear: telecommunications companies should not hand over customer data unless they are lawfully required to do so.

Challenges Facing the New Administration

Maintaining Trust between Business, Government, and Society

We need to align the interests of customers with those of business and government. The experience of Apple versus the FBI might suggest that the interests of industry, government, and society are divergent. We would argue absolutely not. It is about reaching an agreed compromise, a question of balance not absolute choices. Crucially it is about trust and transparency.

Regulation Lags behind Globalization and the Pace of Change

In a globalized information economy, telecommunications companies will often deliver products and services using centralized platforms and infrastructure located across multiple jurisdictions. Regulations that unduly restrict the cross-border transfer of personal and machine-generated data are likely to impede service delivery and distort investment decisions.

The speed of technology change challenges existing regulation. Services come and go rapidly and the development cycle is shortening. Legislation should clearly outline the purpose and offer clarity about the types of government agency who can require access to customer data, along with the process by which that data can be secured. The process should be auditable, and it should be possible, through that audit, to verify that the lawful system is being used.

The Need to Keep Up with Those Who Threaten Our Networks

The scale and changing nature of the challenge are disrupting industry attempts to build internationally compatible safeguards and making it more difficult to have a mature debate with customers about privacy and security.

Recommendations

Incident Reporting and Information Sharing

Following an incident, everyone needs to be clear and precise about what has happened, but government decisions about incident notification and public disclosure of major incidents (or

compliance activities) should not be allowed to disrupt or undermine industry attempts to mount an appropriate and proportionate response.

For the industry to make meaningful headway on standards and standardization, we need to see more intergovernment coordination on standards work to deliver globally accepted outcomes that strike at the heart of the issues.

The telecommunications industry also requires a legal and regulatory framework to promote and uphold technology neutrality and provide a legal framework to encourage investment in future-capable networks that will carry exponentially growing data in virtualized cloud-based environments.

Take a Light Hand with Regulation

Government needs to lead and support national and international conversations required to find the appropriate balance between the need to protect the privacy of the individual and the need to ensure the collective security of society. Policy and regulation must be developed with the specific needs of the enterprise sector in mind rather than as a by-product of regulation designed for consumer needs.

Broaden the Vision of the Public-Private Partnership between Telecommunications and Government

In the digital age, private companies are on the frontline of defense when it comes to cyber threats. Many attacks are not launched at telecommunications companies but through them, in some cases against government or national-security targets. Third parties may struggle to manage the impact of high-level attacks if their prevailing business models don't allow for further investment in cybersecurity. In these situations it might be cost effective for government to use telecommunications companies to provide enhanced security in situations where further investment is needed to reduce the impact of high-level threats and provide a broader common level of defense that it beyond the reach of some organizations but ultimately in the national interest.

Cybersecurity in the Manufacturing Sector

What Makes the Manufacturing Sector Unique

Manufacturers are the creators, users, servicers, and installers of the Internet of Things. This technology is creating enormous opportunity and driving transformative change. It has made all manufacturers into technology companies.

The days of interacting with the customer only during a single transaction are over. Connected technology enables manufacturers to provide real-time performance monitoring and usage patterns for their customers throughout the entire lifespan of a product. A tire manufacturer won't just sell tires but a package to reduce costs through sensors that collect data on fuel consumption and tire pressure.

While connected technology drives innovation in the manufacturing sector, it also creates new challenges. Manufacturers are now the first line of defense in securing our nation's most critical online assets. They place cybersecurity at the highest priority level.

One of the primary targets for cyberattack inside the manufacturing ecosystem is industrial control systems. This is the class of computers that help manage the shop floor. ICS are configured in growing numbers to be reachable through the Internet, including systems retrofitted with modern networking capabilities.

Even when companies take measures to secure their Internet-addressable ICS, they often link their factory production and enterprise information technology networks. That connection results in benefits such as increased productivity, but a new class of malware is exploiting those links to target ICS, likely for espionage.

Challenges Facing the New Administration

The IoT Is Going Faster than Security Can Keep Up

Many IoT devices will possess minimal processing power. That is the nature of the thing—ubiquitous and cheap devices everywhere whose power comes through networking. As a result, many devices may not have capability for basic cybersecurity best practices, such as encryption and operating system updates. Even where capacity exists, manufacturers might not find it economical to patch devices made on a slim margin in a market relentlessly focused on the next generation of products.

Cyber Espionage

Only the government tops the manufacturing sector as a victim of cyber espionage. Espionage isn't just a matter of lost revenue. It's a threat to economic security with implications for national security.

Industrial Control System Security Is underrated

Attackers seeking to disrupt industrial processes don't need to exploit an underlying software vulnerability, the way that sophisticated hackers do when attacking enterprise IT systems. They simply need to gain access to the ICS (perhaps through the corporate IT network) and use the exposed digital controls to manipulate the system into failure. No further hacking required.

The Department of Homeland Security established up in 2009 the Industrial Control Systems Cyber Emergency Response Team in recognition of this challenge, but the years since have proved disappointing. Its main output is further transmitting alerts already widely available to industry.

Recommendations

Incentives for Improving Cybersecurity

Small- and medium-sized manufacturers in particular face bad economics when it comes to achieving a level of cybersecurity robust enough to stand up to nation-states, manufacturing's main cyber threat. This gap between commercially sustainable levels of cybersecurity and what's necessary to counteract foreign adversaries isn't just a market failure. It's the space that federal government was designed to fill by dint of its constitutional charge to provide for the common defense.

What's necessary is a public-private partnership that uses economic tools to encourage investment beyond ordinary levels of commercial cybersecurity spending. Specifically, the government should complete the task begun with creation of the National Institute of Standards and Technology Cybersecurity Framework in determining what the most cost-effective elements of cyber defense are.

Fund IoT Security Research

No amount of incentives can overcome a key characteristic of the Internet of Things: ubiquity of cheap computers with minimal computing power. The ability to seed the environment with cheap computers is what makes the IoT possible.

This is an irreducible problem that requires a different approach to cybersecurity, one premised on building secure systems from insecure components. This isn't a new notion, but it's one that's needs urgent revitalization. The National Science Foundation, the Defense Advanced Research Projects Agency, and the research arm of the Department of Homeland Security should make funding research into this a priority.

ICS-CERT Should Be Strengthened

The Industrial Controls Systems Cyber Emergency Response Team performance needs to enhance its focus on development of best practices and on research. The organization's outreach to the manufacturing sector should also be improved.

"We tend to count things—how many alerts, how many advisories, how many incidents do you respond to," said ICS-CERT director Marty Edwards in May 2016. "I think we have to get to the point of measuring what impact did we make inside of a company, or how is a sector improving or degrading over time in the cybersecurity area," he added. The manufacturing sector concurs.

Cybersecurity in the Food and Agriculture Sector

What Makes the Agriculture Sector Unique

Whether it's wired-up off-road equipment and machinery, high-tech food and grain processing, radio frequency ID-tagged livestock, or global-positioning-system tracking, the agriculture sector depends on information systems to sustain and improve operations, competiveness, and profitability.

Wringing out even more efficient yields is a global and domestic necessity. Population growth and rising living standards will increase future demands for agricultural products. Breadbasket countries like the United States need to find sustained growth in yields and more efficient ways to farm to meet these demands. Without making use of remote sensing and computer science, significant increases in agricultural yields will be impossible.

Embracing technology comes with risks, and the sector finds itself targeted as never before, thanks to its intellectual property being coveted by foreign competitors and hacktivists. Until recently, most food and agriculture companies did not invest in cybersecurity defense and were lax in fortifying their infrastructure and developing sound cybersecurity practices. That's beginning to change.

The delay in grasping the threat wasn't limited to the private sector. In 2010, two federal oversight agencies, USDA and FDA, classified cybersecurity as a low priority. However, in 2015, the agencies reversed course.

This past lack of urgency in the agriculture sector was a mistake, as it missed its chance to get ahead of the threats. All sectors of critical infrastructure are interlaced with dependencies, but the biological requirement of food is arguably at the root of them all. An extreme, coordinated cyberattack on agricultural companies would have human and financial consequences.

Challenges Facing the New Administration

Between the seed seller and the supermarket shopper lies a huge, complex, and volatile supply chain, one of the most complex worldwide. Its components are vastly different in size and sophistication and compete in an economy that optimizes for the lowest possible cost. This level of diversity and size, combined with small budgets for overhead, isn't the best recipe for robust cybersecurity since it results in huge disparities among individual components. As a result, the agriculture sector will be confronted with the same weakest-link problem facing other sectors.

Agricultural production and operations will only increase dependency on software and hardware applications vulnerable to cyberattacks. Smart farm machinery will handle many of the labor-intensive and repetitive jobs still requiring manual work. Smarter, more robust automation will expand into food processing as machines become more apt to deal with irregular size, shape, and quality-control problems.

This new level of connectivity creates vulnerabilities that the sector hasn't fully contended with, especially not in the operational environment. Foreign nations are trying to illegally get ahold of American agricultural technology, particularly data on genetic engineering, improved seeds and fertilizer as well as information related to organic insecticide and irrigation equipment. While most recent cases of intellectual property espionage were done the old-fashioned way, it's naive to assume cyber espionage will not become a major element of commercial espionage.

Prospects of agroterrorism also concern the sector. A sophisticated terrorist attack could wreck America's status as a trusted food exporter and undermine domestic confidence in the food supply chain. The sector's growing digitization brings with it new opportunities for terrorists to attack places that previously have been too remote or difficult to strike. Cyber terrorism is a relatively low-cost venture with high payoff potential, making the risks of agroterrorism too large to ignore.

Recommendations

Increase Awareness

Neither branch of government gives food and agriculture cybersecurity the attention it demands. While new regulations from the federal government are not necessary, agencies that interact with the sector should recognize cybersecurity for the priority issues it has. The FDA and USDA should start educational programs promoting good cybersecurity practices among sector industries.

There is no congressional subcommittee charged with food and agriculture cybersecurity oversight or which deals with communication technology's new dominant role in the sector's growth. Committees within the full House and Senate agricultural committees must be assigned this task.

Define What Constitutes a Nation-State Attack against the Agriculture Sector

Despite widespread attacks by foreign powers, the federal government has yet to define at what point a cyberattack constitutes an act of war or what type of defense it will offer against such attacks. Nor has it updated and adjusted its defense spending in light of this modern threat.

Incentives

Increasing cybersecurity will cost money, and finding the additional funding will not be simple for the sector since it is governed by tight margins and faces a highly competitive world market. Federal involvement in correcting food and agriculture market failures goes back to the New Deal, and this is a new market failure that need correction. Loan forgiveness or grants tied to cybersecurity practices measured against benchmarks such as the NIST Cybersecurity Framework should be implemented, as should new or modified incentive programs for standards, practices, and technologies that are not cost effective but necessary for national security.

Improve Information Sharing

Agricultural cybersecurity information sharing lacks a center. The sector needs a dedicated cyber-threat information-sharing mechanism, designed for chief information security officers at large corporations,

industry associations, and agricultural cooperatives. For smaller, individual enterprises, this mechanism should provide the option of automated updates to threat-protection software. There are plenty of data exchanges dedicated to various threats, such as food-borne illnesses or crop diseases, but cyber gets lost.

Cybersecurity Insurance

Executive Summary

Topics Addressed

Insurance exists to help companies and individuals manage the financial impact of unexpected events. Demand for cyber insurance is rapidly increasing, but take-up rates vary on the basis of company size, industry sector, value of data assets, and regulatory requirements. Companies that purchase cyber insurance generally are buying modest limits.

Challenges

There are several inhibiting factors that constrain its full capacity: Disparate company preparedness and investment; Lack of suitable data for modeling; Challenges of risk aggregation and correlation; Weak public understanding of cyberattack importance; Competing priorities and opportunity costs of insurance purchases; Shortage of qualified talent to address the risk; Rapid growth of the Internet of Things and resultant risks.

Recommendations

Tax Incentives for Cybersecurity Investment: This could take the form of tax incentives for such investments or the purchase of cyber insurance. Companies that partner with cyber insurers have strong economic incentives to continually improve security practices that raise the overall level of national preparedness.

Government Intelligence Sharing: Some Information and Security Analysis Centers are more effective than others, and it would be beneficial to enhance all of them to ensure a consistent level of information and engagement across industry sectors. The federal government can incentivize strong participation by using these forums to deliver timely and highly valuable intelligence on emerging cybersecurity threats.

Scenario Planning Workshops: The insurance industry is prepared to facilitate cross-industry cyber scenario workshops. The workshops would focus on designing and implementing scenario analysis to better understand the types of attacks that could impact the private and public sector.

Clarify the Terrorism Risk Insurance Act: Large-scale terrorist attacks launched by cyber means should qualify as certified acts of terrorism and trigger TRIA for covered lines. Additionally, greater clarity on what constitutes an act of cyber war would be helpful to ensure that all parties are clear if, and when, an event occurs.

Legal and Regulatory Immunity: The federal government should consider legal or regulatory immunity for companies that develop products to prevent and address cyberattacks. The federal government should also consider extending the SAFETY Act to include liability limitations for certified products and services that are designed to prevent or mitigate loss from cyber terrorism and cyber-criminal activity.

Software and Hardware Security Standards: The insurance industry also supports the creation of an independent organization that would be tasked with certifying the security of commonly used software and hardware devices. This initiative would be equivalent to standards developed under the Underwriter Laboratories for the introduction of new electronic devices and components.

The Role of Cyber Insurance in Promoting Cybersecurity

Market Overview

Insurance exists to help companies and individuals manage the financial impact of unexpected events. Demand for cyber insurance is rapidly increasing, but take-up rates vary on the basis of company size, industry sector, value of data assets, and regulatory requirements. Companies that purchase cyber insurance generally are buying modest limits. A recent survey of risk managers suggests that nearly 60 percent buy less than $20 million of coverage.

Cyber Insurance—Product and Service

The insurance industry has created a system to help companies plan, prepare for and respond to incidents. Insurers frequently conduct in-depth reviews of company cybersecurity frameworks during the underwriting process. Insurers also offer a suite of ex-ante and ex-post services that minimize the likelihood and impact of a breach.

Market Challenges

While the market is advancing quickly, there are several inhibiting factors that constrain its full capacity:

- Disparate company preparedness and investment.
- Lack of suitable data for modeling.
- Challenges of risk aggregation and correlation.
- Weak public understanding of cyberattack importance.
- Competing priorities and opportunity costs of insurance purchases.
- Shortage of qualified talent to address the risk.
- Rapid growth of the Internet of Things and resultant risks.

Recommendations

Tax Incentives for Cybersecurity Investment

This could take the form of tax incentives for such investments or the purchase of cyber insurance. The latter would ensure that more companies are subjected to an independent review of their cybersecurity

framework. Companies that partner with cyber insurers also have strong economic incentives to continually improve security practices that raise the overall level of national preparedness.

Government Intelligence Sharing

Some Information and Security Analysis Centers are more effective than others, and it would be beneficial to enhance all of them to ensure a consistent level of information and engagement across industry sectors. While participation in such groups is voluntary, the federal government can incentivize strong participation by using these forums to deliver timely and highly valuable intelligence on emerging cybersecurity threats.

Scenario Planning Workshops

The insurance industry is prepared to facilitate cross-industry cyber scenario workshops. These would involve federal government agencies, universities, corporations, and other participants. The workshops would focus on designing and implementing scenario analysis to better understand the types of attacks that could impact the private and public sector.

Cybersecurity Education

The government's program to certify universities and provide loan forgiveness to students who major in cybersecurity and work for the government is a very good start. We recommend continuing to invest in such programs to ensure that a suitable pool of talent is filled and that companies can draw on this pool. Federal funding for research at nonprofits and universities would also dramatically improve the level of knowledge in the field.

Public Service Campaign

We also recommend creating a public campaign similar to the "Say No to Drugs" campaign. Additionally, educational materials should be developed and delivered to midsized and small businesses through various channels such as the Small Business Administration and other governmental programs.

Geopolitical Risk Management

Companies are incapable of protecting against sophisticated, well-funded nation-state attacks. As such, the DHS, FBI, and NSA need to take the lead in protecting the country against such attacks through appropriate offensive and defensive means. Further, intelligence gained from such actions should be shared openly with the private sector to enhance understanding of threats and allow for preparedness.

Clarify the Terrorism Risk Insurance Act

Large-scale terrorist attacks launched by cyber means should qualify as certified acts of terrorism and trigger TRIA for covered lines. Additionally, greater clarity on what constitutes an act of cyber war would be helpful to ensure that all parties are clear if, and when, an event occurs.

Legal and Regulatory Immunity

The federal government should consider legal or regulatory immunity for companies that develop products to prevent and address cyberattacks. The federal government should also consider extending the SAFETY Act to include liability limitations for certified products and services that are designed to prevent or mitigate loss from cyber terrorism and cyber-criminal activity.

Software and Hardware Security Standards

The insurance industry also supports the creation of an independent organization that would be tasked with certifying the security of commonly used software and hardware devices. This initiative would be equivalent to standards developed under the Underwriter Laboratories for the introduction of new electronic devices and components.

Cybersecurity Research and Development

Executive Summary

Topics Addressed:

Current and future trends: The nascent Internet of Things promises to make homes comfortable and vehicles safer. Connected devices make offices more efficient and drive down energy costs. They increase crop yields and monitor pipelines. The IoT will make services like predictive maintenance a standard offering, as well as enable efficiencies and flexibility across the entire manufacturing process and down the supply chain that feeds it. Productivity could go up by as much as 30 percent.

Current and future trends: While products to protect information technology infrastructure are readily available and mature (e.g., firewalls, intrusion-detection system, and incidence and event management systems), there are far fewer products in the marketplace that provide security for the highly connected operational technologies that control physical assets on the power grid.

Challenges:

Operational technology: Utility asset vendors sell closed-source devices and software solutions, which typically come bundled with significant contractual prohibitions against tampering or reverse engineering. This results in a difficult situation, preventing utilities from processes that might allow them to verify the integrity of hardware and software they purchase. In addition, it creates an impractical hurdle for utilities preparing response plans for cyberattacks such as by running war games premised on maliciously tampered-with devices or software, a reality that occurred in Ukraine.

Recommendations:

Fund IoT Security Research: A key characteristic of the Internet of Things will be the ubiquity of cheap computers with minimal computing power. The ability to seed the environment with cheap computers is what makes the IoT possible. Durable goods will likely possess sufficient capacity for cybersecurity measures such as firewalls. But they will be the exception. What makes the IoT possible is also what makes it vulnerable.

This is an irreducible problem that requires a different approach to cybersecurity, one premised on building secure systems from insecure components. This isn't a new notion, but it's one that's needs urgent revitalization, forearmed as we are with the certain knowledge of a planet's worth of devices coming online in the near future. The National Science Foundation, the Defense Advanced Research Projects Agency and the research arm of the Department of Homeland Security should make funding research into this a priority.

Promote Innovation through Government Grants: The government should fund grants and cooperative agreements in support of commercial product development for operational technology used in critical infrastructure, particularly in the local distribution electric grid. Initiatives such as Rapid Attack Detection, Isolation and Characterization Systems at the Defense Advanced Research Projects Agency and Cybersecurity for Energy Delivery Systems at Energy encourage investment in commercial products by appropriately reducing risk for potential vendors and helping bring together all relevant stakeholders. These programs should be continued and expanded.

Cybersecurity Workforce

Executive Summary

Topics Addressed:

The deficiencies in the cyber workforce are troubling and vexing. There is an apparent market failure wherein we have an exciting, modern field with lots of high paying jobs that we can't fill, and this deficit is expected to continue for some time. Meeting the nation's cybersecurity challenge will require a multipronged effort. Sustained investment in research and innovation, successful implementation of new models for public-private collaboration, and the continued advancement of incentives that spark continued private-sector investment in cybersecurity capabilities are all vital components of an effective strategy

Challenges:

The increasing demand will be driven by the collision of bits and atoms disrupting a host of industrial sectors. The rapid convergence of wireless technologies, sensors, microelectronic systems, and the web—the rise of the Internet of Things—is dramatically increasing the need for cybersecurity skills. Connected devices bring new threats, vulnerabilities, and the imperative for new approaches to security, because securing IoT devices demands strategies fundamentally different than locking down personal computers or mobile devices.

Recommendations:

We need to reach kids where they are and integrate cybersecurity into what they want to do, not teach them what they ought to do. One neglected vehicle is the gaming community. Gaming events can encompass hundreds of thousands of online players and spectators. If cybersecurity could be integrated into these events, it might be a pathway to reach tech-interested youths, which could be complimented by camps and contests where the notion of developing a career doing what they already like could be planted.

Career influencers, including high-school guidance counsels (who are generally unaware of the profession), at community colleges and universities need to be reached with messaging targeted to these particular audiences at this particular stage of their lives.

Expand the scholarship for service program and foster even deeper cross-institutional collaboration. One model for such an effort is the Cyber Stakes program, which has fostered collaborative education and exercises between Carnegie Mellon and service academies. Explore creation of a cybersecurity rotc program. A cyber-specific ROTC-like initiative would underscore the sense of national mission that is vital to addressing the environment for strengthening the cybersecurity talent pipeline. A key to this effort would be to create a strong network among institutions operating this program to ensure that the development of these students included both deep technical and operational experiences.

Additionally, consideration should be given to development a "2+2" model for this effort, where a student who has a potential interest in cybersecurity can receive a modest financial-aid supplement in their first and second year.

Workforce Development: Awareness Yields to Understanding and Makes Cybersecurity Cool

The deficiencies in the cyber workforce are not only troubling but also vexing. There is an apparent market failure wherein we have an exciting, modern field with lots of high paying jobs that we can't fill, and this deficit is expected to continue for some time.

The new administration must aggressively move away from antiquated development models based on single-month programs, school curriculum development, and TV spots. The reality is the average fifth grader probably knows more about technology than the average fifth-grade teacher. Teachers will tell you they don't have time to teach civics or geography, so adding cybersecurity to the mix is unlikely to have an impact.

We need to reach kids where they are and integrate cybersecurity into what they want to do, not teach them what they ought to do. One neglected vehicle is the gaming community. Much as the government has reached out to IT companies in Silicon Valley, a similar collaboration should commence with game developers. Cybersecurity principles and techniques could be integrated into an activity young people easily gravitate toward.

Gaming events can encompass hundreds of thousands of online players and spectators. If cybersecurity could be integrated into these events, it might be a pathway to reach tech-interested youths, which could be complimented by camps and contests where the notion of developing a career doing what they already like could be planted.

A few young cyber stars might put a face on the activity that others could relate to. It might also be possible to leverage television. Just as ESPN turned niche activities like poker and fantasy football into

extremely popular portions of their lineup, the same could be done with gaming with a cyber component.

At another level there ought to be highly targeted outreach to opinion makers. It is critical that diverse populations of young people are recruited to be part of helping design the outreach effort toward diverse audiences. Charismatic, young adult cyber professionals can be recruited to use social media like forums, blogs, Snapchat, Instagram, and YouTube to build followings talking about how interesting, lucrative—and fun—the career path can be. Again an emphasis on developing "stars" that can put diverse faces on the field need to be cultivated.

Career influencers, including high-school guidance counselors (who are generally unaware of the profession), at community colleges and universities need to be reached with messaging targeted to these particular audiences at this particular stage of their lives.

Industry, which is already operating a multitude of one-off outreach programs, should be urged to collaborate so that consistent messaging reaches as broad a population as possible in an effort to secure the ecosystem as opposed to a particular company.

Given limited resources, the new administration ought to make government's primary mission to coordinate with the private sector on its programs, as opposed to developing independent government programs (apart from government recruitment as discussed in later chapters). Government can open doors, facilitate partnership, and allow the private sector to be the major creators and operators of the workforce-development program.

One high-value area wherein government can take a direct role is doing a better job educating itself. A higher-value target for cyber education than K–12 might well be the House and Senate. Most senior government officials are digital immigrants not born into the digital world they inhabit—but nonetheless charged with establishing governance over systems they understand poorly.

Senior government officials (members of Congress, cabinet secretaries, and agency heads) can aptly compare to corporate board members in terms of status, responsibility, and cramped schedules. Senior government officials have for years campaigned to have corporate boards become more educated about cybersecurity so they could better manage it.

As detailed in chapter 12, the National Association of Corporate Directors has over the past few years taken up that challenge and developed a very well received handbook and education program. PricewaterhouseCoopers in its 2016 Global State of Information Security has documented that this effort has yielded significant real worked effect including increasing budgets for cybersecurity by 24 percent, fostering better risk management, creating a culture of security, and engendering better communication about these issues within the enterprise.

Clearly the federal government could use this kind of assistance. We ought to do the same thing for the government equivalents of corporate board members as we are already doing for our commercial directors.

The new president should insist that all senior government officials (not the IT people—they already get it) take a cybersecurity-training program based on the NACD model. Congressional leaders and independent agencies should follow suit.

Winning the Cyber-Talent War: Strategies to Enhance Cybersecurity Workforce Development

Examining Progress to Date in Efforts to Strengthen the Cybersecurity Workforce

A Partnership for Building the Future Public-Sector Workforce—the Scholarship for Service Program

Funded by the National Science Foundation and operated in partnership with DHS, the Cyber Corps of the Scholarship for Service program has demonstrated significant impact in encouraging students to pursue cybersecurity careers and creating a pipeline of talent for the public sector.

National Centers of Academic Excellence in Cyber Defense

This program sets criteria and mapping curricula to assist institutions in building effective cybersecurity education and research programs—helping to establish a national framework for cybersecurity education. All four-year baccalaureate, graduate education, and two-year institutions are eligible.

Presidential Innovation Fellows

The fellows program is designed to engage early career IT professionals and engage them in short stints in government. While not focused exclusively or even predominantly on cybersecurity, the Presidential Innovation Fellows program provides a window on a future where an improved flow of critical cybersecurity talent could be a vital resource for meeting major short-term challenges and raising the overall level of skills in the cyber workforce.

National Guard and Military Reserve Cyber Operations

Regional centers being developed by the National Guard and Reserve are creating a nexus of talent within states and cities that draws on professionals engaged in industry and academia who can be mobilized to support government needs in the case of major incidents.

Engaging Veterans in Cybersecurity Careers

A number of promising initiatives have also been launched in the last few years to focus cybersecurity education on veterans. These efforts include specific outreach and degree programs—including those launched by the state of Virginia and boot camp programs launched by companies such as PricewaterhouseCoopers, among others.

Initial Steps to Nurture Cybersecurity Career Paths for Young Americans

As part of the National Initiative for Cybersecurity Education (more often known as NICE), federal agencies collaborate to strengthen K–12 student and teacher engagement. One of the leading examples of this effort is the GenCyber initiative supported by NSF and the NSA. GenCyber supports collaborations with academic institutions to conduct cybersecurity summer camps for students and teachers.

Shaping an Agenda for the New Administration: Principle Building Blocks of an Effective National Cyber Workforce Strategy

Focus a National Initiative on Building the Talent Pipeline

Attracting students into the federal government must be augmented by an aggressive strategy to build the pipeline of interest in earlier grade levels. This will require a broad range of engagement with K–12 education that includes classroom initiatives, expanded teacher education, and after-school competitions to spark interest.

Embrace the Positive Elements of the Hacker Dynamic

Hackers are ultracurious, highly imaginative professionals who are able to spot even the most hidden vulnerabilities in systems. Meeting the nation's cybersecurity talent needs will require nurturing the natural curiosity and imaginative creativity that defines the hacker experience.

Create New Vehicles for Industry, Government, Education Collaboration

While policies to date have focused on the needs of the federal government, the national cybersecurity workforce is a challenge for the private sector as well. Opportunities must be explored to foster closer coordination among government, industry, and the higher-education community as the nature of the cybersecurity challenge evolves.

Policy Recommendations for New National Federal Cybersecurity Workforce

Intensify Initiatives to Create a Cyber-Aware Generation

Incorporating basic cybersecurity education into curricula at all education levels and work experiences would enhance this first line of defense. Along with this effort, we need to invest in research and applied development of innovations that continue to make security and privacy easier for consumers.

Develop a Core Cybersecurity Curriculum That Can Be Adapted and Applied at All Education Levels and Start Building Cybersecurity into STEM Programs

Recognizing the importance of cybersecurity as a fundamental element of STEM education will also enhance the growth of programs and stronger student interest.

Engage Industry and the Higher-Education Community in Commitment to Train One Hundred Thousand High-School and Middle-School Teachers in Basic Cybersecurity Education in the Next Five Years

This component can tap the development of new online and gamification tools that have the potential to significantly impact the ability to bring cost-effective education resources to schools throughout the nation. Carnegie Mellon experienced the success with picoCTF, and nationwide adoption of this model, specifically aimed at educators who can run their own versions of the contest, could have an exponential impact.

Using the FIRST Robotics League as a Model, Advance a National Strategy for Middle-School and High-School Hacking Contests to Excite the Next Generation of Cybersecurity Professionals

Now in its twenty-fifth year, FIRST reaches seventy-five thousand students around the world each year and provides a broader portal to STEM careers. A national hacking contest initiative can have a similar impact.

Expand the Scholarship for Service Program and Foster Even Deeper Cross-Institutional Collaboration

The proposal to increase the number of institutions in the program is a valuable component of a talent initiative. One model for such an effort is the Cyber Stakes program, which has fostered collaborative education and exercises between Carnegie Mellon and service academies.

Explore Creation of a Cybersecurity ROTC Program

A cyber-specific ROTC-like initiative would underscore the sense of national mission that is vital to addressing the environment for strengthening the cybersecurity talent pipeline. A key to this effort would be to create a strong network among institutions operating this program to ensure that the development of these students included both deep technical and operational experiences.

Additionally, consideration should be given to development a "2+2" model for this effort, where a student who has a potential interest in cybersecurity can receive a modest financial-aid supplement in their first and second year. At the end of the second year, these students (and any other students in the program) can choose to apply for acceptance into a program fully funding their tuition during the third and fourth year, if they commit to a cybersecurity minor in addition to their computer science or electrical and computer engineering major. In return, the student would be required to sign up for three years of service in a government cybersecurity position.

Create New Mechanisms for Industry, Government, Higher Education Collaboration

One strategic approach to fostering these new mechanisms would be to support the development of regional test beds for collaboration on the emerging Internet of Things. These test beds could focus both on innovation in cyber applications and advancing opportunities for formal education programs as well as ongoing training initiatives.

Identity and Access Management

Topics Addressed:

The realities of today's cyber-threat environment have resulted in the widespread leakage of Americans' sensitive information, thanks to a data-breach epidemic. For consumers, the fallout has been an upswelling of identity theft and account takeovers. And as a result, the security model of identity authentication by user ID and password, including the use of "security questions," is no longer acceptable. Increasingly, financial institutions and other online entities require more effective methods of achieving online authentication without an undue level of inconvenience.

Challenges:

"Killing the password" has been a long-standing Obama administration priority, one that it reiterated in the National Cyber Action Plan unveiled in February 2016.

We enthusiastically support moving consumer authentication from traditional passwords to one of "multifactor authentication"—as also recommended by the Federal Financial Institutions Examination Council in its 2005 guidance on authentication in Internet banking environments. But we're concerned that enthusiasm for supplanting passwords with alternatives such as facial or fingerprint recognition isn't translating into results, despite high-level support from the administration. Although it launched in 2011 a program called the National Strategy for Trusted Identities in Cyberspace charged with creating market conditions favorable to a wholesale replacement of passwords, it's clear today the effort has stalled.

Partial fault lies with NSTIC and its private-sector stakeholders, which bogged down the effort in inward-facing debates over governance. Blame goes to Congress too, which has cut NSTIC funding and treated it as a political football for scoring points during the appropriations process.

Recommendations:

We'd like NSTIC to accelerate its output and do so with the full support of Congress. In addition, the rollout of multifactor authentication for government websites, such as tax-related sites operated by the Internal Revenue Service, is far overdue.

We also urge the National Institute of Standards and Technology to continue its engagement with the Fast Identity Online Alliance, an industry consortium for developing standards for identity authentication. The alliance, known as FIDO, is making it possible for the private sector to build innovative new ways for consumers to validate their identities by publishing widely adhered-to technical standards. NIST's decision to join the alliance in June 2015 is laudable and the next administration should ensure the agency remains actively engaged.

Internet of Things

Topics Addressed:

The IoT Is Going Faster than Security Can Keep Up: Although in its infancy, the Internet of Things is already a target of cyberattacks. Symantec identified in 2013 a worm apparently engineered to attack devices such as television set-top boxes. Although the report was later debunked, one cybersecurity firm made waves when it claimed to have uncovered a smart refrigerator used by attackers to send out spam. The mere fact that a household appliance may be a target has elevated the level at which manufacturers must consider securing the IoT.

Challenges:

Many IoT devices will possess minimal processing power. That is the nature of the thing—ubiquitous and cheap devices everywhere whose power comes through networking. As a result, many devices may not have capability for basic cybersecurity best practices, such as encryption and operating system updates. Even where capacity exists, manufacturers might not find it economical to patch devices made on a slim margin in a market relentlessly focused on the next generation of products.

Devices are only one part of the IoT universe. Databases holding telemetry generated by the devices are another substantial component, one that likely to become another target for hacking. Cybersecurity firm iPower Technologies already spotted in 2015 malware targeting newly purchased police body cameras, likely in order to access law-enforcement data.

Recommendations:

Market forces stymie private-sector businesses from standing up cybersecurity capacity beyond the threshold of normal commercial risk, forces which are particularly strong for small- and medium-sized businesses. This gap between commercially sustainable levels of cybersecurity and what's necessary to counteract foreign adversaries isn't just a market failure. It's the space that federal government was designed to fill by dint of its constitutional charge to provide for the common defense. What's necessary is a public-private partnership that uses economic tools to encourage investment beyond ordinary levels of commercial cybersecurity spending.

Specifically, the government should complete the task begun with creation of the National Institute of Standards and Technology Cybersecurity Framework in determining what the most cost-effective elements of cyber defense are. The executive order that resulted in the framework's creation never saw it as an end in of itself. The order charged the network with setting out a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to cybersecurity (emphasis added).

For NIST to determine how to use the framework cost-effectively is, admittedly, no easy task. But the structure for setting up studies with private-sector cooperation already exists with the sixteen critical infrastructure sector coordinating councils and their sibling government coordinating councils. In a nutshell, the councils for each critical infrastructure sector should seek out representative companies and solicit their voluntary participation in studies to test practical application of the framework in their information technology infrastructure. The studies would measure costs and benefits and identify where the chasm between commercially sustainable cybersecurity protections and nation-state-level protections opens up.

Public Awareness and Education

Topics Addressed:

While a decade ago there may have been a need for a cybersecurity awareness program, we are well past the awareness stage.

Challenges:

The antiquated notion of October being the “Cyber Awareness Month” is illustrated by its slogan, “Stop, Think, Connect,” which hails from the dial-up era. Virtually everyone is now connected twenty-four seven, and cyber awareness needs to equally practiced all the time.

Recommendations:

We now need a program focused not on awareness but on understanding the issue. We need a second targeted set of programs focused on recruiting people to help fill the cybersecurity workforce void, which like the issue itself, goes beyond technical expertise and runs to overall risk management.

Instead we need an integrated, multifaceted, and targeted program with research-based messaging, just as the private sector would do when marketing any product or service.

We recommend creating a public campaign similar to the “Say No to Drugs” campaign. This would be highly effective in raising the general level of awareness for cybersecurity and raising the issue to national attention. Additionally, educational materials should be developed and delivered to midsized and small businesses through various channels such as the Small Business Administration and other governmental programs. We recommend that the federal government partner with leading universities to develop the content for the campaign and the release of such materials.

Additional Topics

Executive Summary

In response to the Commission's request for input on 1. Economic and other incentives for enhancing cybersecurity; 2. Government-private sector coordination and cooperation; and, 3. The role(s) of the government in enhancing cybersecurity for the private sector, we offer the following four sets of comments.

This first two sets co comments outline the recent history of US policy development in cybersecurity and explain how the legacy models developed in the 19th and 20th centuries such as government mandates, prescriptive regulation and punitive liability are ill-suited to address the 21st century issue of cybersecurity.

Moreover we trace the evolution of US cyber policy illustrating that these historic models, with few exceptions, have been found to be inadequate on a bipartisan basis.

The ISA is troubled by reports that the Commission may be suggesting a rehash of these outdated approaches.

It is vital that the Commission build on public-private partnership platforms erected through efforts such as President Obama's Cyber Space Policy Review, the House GOP Task Force Report, Executive Order 13636 and the NIST Cybersecurity Framework.

Given the immediacy and urgency of the threat we simply don't have time to resurrect obsolete structures and attempt to apply them to issues they were never designed to address. We're like Medieval potentates dealing with the arrival of gun-powder. Mandating deeper moats and thicker walls will not work. The Commission must look forward, not backward.

In keeping with the consensus approach developed ISA, we offer a 12-step program for the Commission to consider. The program's recommendations range from the tonal approach next administration should adopt (e.g. we need to act with greater urgency and spend more money) to the strategic (we need to better integrate economics into cyber policy and focus more on smaller companies, to the operational (e.g. we need to develop metrics for the NIST framework and reform cyber audits).

The next section of comments addresses what exactly we mean when we talk about public-private partnerships and reports on joint industry and DHS research that outlines best practices for running these partnership programs in ways that will yield the most success.

The final section of comments addresses the issue of developing mechanisms to assess our progress in strengthening our nation's cybersecurity. We offer a specific and fairly detailed proposal that builds on the model embedded in the current National Infrastructure Protection Plan and leverages the NIST Framework to fully implement EO 13636.

A Brief History of the Cybersecurity Problem and Policies That Have Attempted to Address It

The Problem: It's Really Bad—and about to Get Much Worse

The Internet was designed in the '70s and '80s to be an "open" system, not a secure system. The core protocols that the Internet is based on are insecure by design. In addition, new software services and applications tend to be built on these core protocols, and so modern innovative products inherit the original vulnerabilities. This trend will be exacerbated by the explosion in mobile devices and the Internet of Things.

The Attack Community Is Growing Much More Sophisticated

Nearly a decade ago, the National Security Agency coined the term "advanced persistent threat." APT was originally used to describe the ultrasophisticated, multistaged cyberattacks we had begun to see between nation-states and the defense establishment. We are now seeing these same sorts of attacks being launched throughout the cyber ecosystem. The advanced persistent threat has now become the *average* persistent threat.

All the Economic Incentives in Cybersecurity Favor the Attackers

When one considers the economic balance—the cost benefits of cybersecurity—it quickly becomes apparent that the economic balance overwhelmingly favors the attackers. Cybercriminals have an extremely attractive business model. Unlike many traditional illicit enterprises that require the use of a large, unreliable workforce, and long supply chains, cyberattacks require comparatively small workforces that can be safely located far from disruptive civil forces. Attackers generally have first-mover advantage in deciding who, when, and how to attack, often on the basis of stealthy reconnaissance. Defense is historically a generation behind the attacker. Complicating the economic

imbalance, many of the technologies and business practices that are required for enterprises to operate successfully in a worldwide competitive market tend to undermine cybersecurity.

Why Traditional Mechanisms Are Failing to Provide Security

They Were Designed for a Different Type of Problem

Traditional mechanisms such as independent regulatory agencies, consumer lawsuits, and government regulation are proving ineffective in adequately bolstering our security in light of the modern threats. Much of our traditional regulatory processes and judicial enforcement are designed to address malfeasance. However, the core problem with cybersecurity is not that the technology is poorly constructed or companies are unwilling to invest in reasonable security. It's that the technology is under attack.

Government Doesn't Have the Credibility Needed to Regulate for Cybersecurity

There is no evidence that government has attained that degree of expertise in cybersecurity. In fact, the data suggest the opposite. Greg Wilshusen, director for info security at the Government Accountability Office, explained in congressional testimony some of the reasons why. Among them is this:

"Government agencies follow what IT pros call a policy-based approach to cybersecurity where agencies check off a list of requirements set by lawmakers and regulators that they have to follow."

Government Is Not Properly Structured to Deal with the Digital Age

A Bank of America Merrill Lynch 2015 report found that "The US government is still in the process of determining who will have jurisdiction in cyberspace. As the Department of Defense, DHS, and their subordinate organizations like the Air Force, Navy, Army, Defense Agencies and Commands battle for jurisdiction and funding. The result is a fragmented system muddled with a political agenda which hinders the development of a more secure system."

Even If Government Were Up to the Task, the Regulatory Model Doesn't Fit the Problem

The expert agency regulatory model, wherein an elected body empowers a regulatory agency to specify requirements for the private sector, essentially attempts to locate a static standard that assures safety wherever producers are in compliance. Technology and attack methods change constantly and quickly. The traditional regulatory process cannot keep up with the evolution of what constitutes the required cybersecurity at any given time.

There is a role for regulation in certain spaces, such as requirements to notify citizens when their personal data have been compromised, or in industries where the core economics of the industry are already intimately involved in regulation, such as municipal water services. But traditional regulation generally falls short as an effective sustaining private-sector cybersecurity, because of the nature of government and the nature of the problem itself.

Other Industrial-Age Control Mechanisms Are Not Working, Are Inappropriate, and May Be Counterproductive

Disclosure Models Don't Fit the Digital Age

While citizens have an obvious right to know if their personal data have been compromised (as virtually every state now demands), disclosure as a motivator for improved security is too blunt an instrument to achieve our broader goals.

Court Action Is Proving Ineffective

Notwithstanding the hype from the plaintiff's bar, the predicted (for ten years) avalanche of lawsuits by consumers harmed by cyberattacks and the resulting improvements in security to avoid such suits has not materialized. One of the main reasons for this mechanism's failure to promote the needed security upgrades is that the suits are usually unsuccessful.

The Path Forward: The Cybersecurity Social Contract

The concept of the social contract initially focused on the relationship between the individual and the state and what each would exchange with the other in order to achieve broader social order and benefit for the community. In the early twentieth century, the social contract was adapted to the exchange between corporations and the state in order to achieve mutual and greater benefit for the social order.

At the time, the hot technologies were telecommunications (phones) and distributed electricity. Initially these services were provided where the economies justified them: urban and affluent areas. The policy makers of the era understood that universal service of these technologies would have broad social benefit but also realized government couldn't accomplish this on its own. Moreover, compelling the private sector to provide the services without adequate compensation would be an unsustainable model.

So, a "social contract"—essentially an economic deal—was developed. Private companies agreed to provide universal service at regulated rates. In exchange, the government agreed to guarantee a substantial rate of return on their investments. Thus was born rate-of-return regulation and the private-investor-owned public utility.

Critical to understanding the social contract as applied to infrastructure development in the United States is the realization that not only did it enhance the greater public good but there was also an economic exchange in return for this societal benefit. Moreover, the infrastructures, adequately supported by the economic incentives imbedded in the contract, were continually made more sophisticated and innovative. The rapid development of these infrastructures provided the foundation for accelerated industrialization, job creation, and innovation.

In publications printed in 2008 and 2009, ISA argued that a similar situation exists today with respect to cybersecurity. In the ensuing years, we have seen substantial progress at the conceptual level as the

private sector and both political parties have gravitated toward embracing the Cyber Social Contract model.

President Obama's signature policy paper on cybersecurity, "Cyberspace Policy Review," authored by Melissa Hathaway, made ISA's 2008 "Cybersecurity Social Contract" publication it's first and most frequently cited reference. In 2013, the president issued an executive order on cybersecurity that also embraced the principles of the cyber social contract. The president abandoned the traditional regulatory approach and instructed the National Institute of Standards and Technology to identify the appropriate standards and practices that ought to be voluntarily adopted by the private sector and reinforced by the development of market incentives.

Although we have now developed a broad consensus on the conceptual approach, we need to stimulate progress on implementation. As we turn to a new administration and Congress, there is still a great deal of work to be done, at both the macro- and micro level, to build on the consensus that has been developed and implement a secure cyber system that is both technologically responsive to the evolving threat and economically sustainable.

Twelve-Step Program for Implementing the Cybersecurity Social Contract

1. We Need to Attack the Cybersecurity Problem with Much Greater Urgency

Compared to the speed with which our information technology systems are being compromised, federal policy making has moved at a glacier pace, because of bureaucratic processes and constant turf battles. A new president can do a lot to set the proper aggressive tone to address the issue. Cybersecurity needs to figure prominently in the new president's first hundred-day agenda.

2. Government Needs to Recognize the Importance of Economics in Cybersecurity

In cybersecurity virtually all economic incentives favor the attacker. Attacks are cheap, easy to access and immensely profitable. Defense is hard, reactive and it's hard to show ROI to what you have prevented. Research continually shows that cost is often the principle obstacle to improved cybersecurity yet government answers to cyber issues is typically to throw more IT at it. Cybersecurity is not a technical issue. It's an enterprise wide risk management issue with a technical component. The new administration needs to expand the focus on cybersecurity beyond the IT silo, and rebalance the economic-incentive structure.

3. Government Needs to Dramatically Increase Funding for Cybersecurity

Improving cybersecurity will cost money. Estimates of the cost of cybercrime run to a trillion dollars a year. Non-defense government spending for cyber is about $9 billion, going up about 9% a year. Private sector spending on cyber is about $120 billion going up 24% a year. Two commercial banks currently spend more annually on cyber than the entire Department of Homeland Security. Government must invest far more in cybersecurity.

4. Government Needs to Be Organized to Reflect the Current Digital Realities

Now, well into the digital age, our government is still organized on an industrial age model. This creates gridlock and massive inefficiency. There are 87 different congressional committees with jurisdiction over cybersecurity. Government itself needs to be modernized. The incoming administration needs to reorganize for the digital age, and government needs to fully integrate the private sector into its cybersecurity planning and operations.

5. We Need to Focus More on Cybersecurity from a Law-Enforcement Perspective

We successfully prosecute less than 2% of cyber criminals. Law-enforcement agents are vastly overmatched and under-resourced. The legal structure, particularly internationally, has not adapted to deal with modern cybercrime. The new administration should engage in a multi-tiered program to

bolster cyber law enforcement, review legacy law-enforcement spending, and help create a practical, operational international legal structure to address international cybercrime.

6. Test Pilot the NIST Cybersecurity Framework

No private-sector organization launches a new product or service without testing it yet nearly 3 years since its release we have not a single piece of objective data to show that the NIST Framework has changed behavior, that any changes have improved security or that they are cost effectiveness. Executive Order 13636, directed that the Framework be prioritized and cost effective, yet virtually nothing has been done to objectively demonstrate this. If the voluntary Framework system is to survive it must be supported by data. Companies will, naturally use systems that have been shown to be cost effective and small companies in particular need a prioritized Framework that is more practical for them to use.

7. Government Should Prioritize Helping Smaller Companies

Smaller companies are more vulnerable than larger ones, understand the issue less, are investing less, and are probably the segment that most needs government help. Small companies are used as access points for sophisticated attacks on larger firms. We cannot develop a sustainably secure system by focusing exclusively on large companies. Government must increase its emphasis on smaller companies, and make cybersecurity easier and cheaper for SMBs.

8. We Need a More Creative Approach to Workforce Development:

We need an integrated, multifaceted, and targeted program with research-based messaging. Career influencers, such as school counselors need to be targeted with proper messaging. We should use the gaming community to attract kids, and integrate cybersecurity into existing games –make cyber cool. Government should focus on training at the top. The National Association of Corporate Directors operates a highly successful training program for corporate boards that has been empirically verified to

be successful. We need a similar training program for the government equivalent of corporate boards (Members of Congress, agency heads, etc.)

9. Modernize and Streamline Regulation

The NIST Framework is supposedly a voluntary program yet since its inception we have an explosion of cyber regulations. Companies now often face multiple inconsistent regulatory and quasi-regulatory "NIST-based" systems that are driving up costs while diverting scarce resources away from security to focus on compliance. The new president ought to develop a cross-government program for streamlining regulations. Congress should aggressively require federal agencies to reduce duplicative regulations and eliminate those that have not been proven to be cost effective as a condition of their annual appropriations.

10. Develop Market Incentives to Promote Sound Cybersecurity Behavior

Both the House GOP Task Force Report on Cybersecurity and President Obama's EO 13636 called for the development of market incentives to promote cybersecurity. Yet, other than the recently enacted information sharing bill there has been virtually no work done in on developing incentives. Policy makers The private sector has offered over a dozen incentive models for consideration including liability incentives, procurement incentives, insurance incentives, and good actor benefits such as streamlined regulation, patent or trademark preferences, forbearance, and streamlined auditing, yet there has been virtually no legislative consideration to date.

11. Articulate Clearly the Role for Government When Industry Faces a Nation-State Attack

Many cyberattacks are affiliated with nation-state actors. Virtually no private institution can adequately defend itself from a concentrated nation-state attack. There is no clear policy or systemic assistance private companies can expect from the federal government when dealing with nation-state cyber

threats. The federal government should offer (on request) equivalent federal assistance to private companies that suffer a cyberattack by a nation-state as if it were a physical attack.

12. Government and Industry Need to Partner to Rethink the Cybersecurity Compliance Model

The traditional regulatory model is ill-suited to the cyberspace. We need to create a forward-looking, risk-management model powered by growth and incentives, not penalties and compliance. The new administration must work collaboratively with the private sector to develop this model.

Best Practices for Cybersecurity Public-Private Partnerships

Introduction

President Barack Obama has said,

> The federal government cannot succeed in securing cyberspace if it works in isolation. The public and private sectors interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure upon which businesses and government depend…Only through such partnerships will the United States be able to enhance cybersecurity and reap the full benefits of the digital revolution.

However, despite years of attempting to conduct cybersecurity programs in partnership, it's become apparent that not only were most partnership programs unsatisfying to both parties but even the definition of partnership is also unclear. This confusion and frustration was seen as endangering the partnership model or redefining it in such a way as to rob it of its novel approach to security.

This chapter identifies a set of best practices for operating cybersecurity public-private partnerships on the basis of a collaborative research project conducted jointly by the IT Sector Coordinating Council and DHS staff.

Method

The government and industry investigators used a modified critical-incident methodology to examine a range of joint programs ostensibly run under the partnership model as identified in the National Infrastructure Protection Plan.

Acting separately, the government and industry groups independently evaluated the various projects on a success scale. Both government and industry evaluators determined that same projects to be successful and less successful.

The groups then undependably identified a set of practices that in their expert opinion as practitioners in the field made the programs successful or not. Consensus was reached as to what practices accounted for the success of the projects.

The case studies that were used for this analysis included

- the 2006 development of the National Infrastructure Protection Plan,
- the IT Sector Baseline Risk Assessment,
- the construction of the "Cyberspace Policy Review,"
- industry integration into the National Infrastructure Coordination Center,
- the IT Supply-Chain–Risk-Management Collaboration, and
- the development of the "Blueprint for a Secure Cyber Future."

Results

Both industry and government evaluators agreed on a dozen best practices that tended to generate successful partnership programs in cybersecurity. These are as follows:

- Senior-level commitment to the partnership process communicated to staff and upper echelons.
- Involvement at the priority, goal, and objective phases of projects, not just implementation.
- Use of the process identified in the NIPP for involving industry.
- Reaching out to stakeholders early on, ideally at the "blank page" stage.
- Continuous and regular interaction between government and industry stakeholders.
- Providing adequate time for stakeholder review (equivalent to government review).
- Establishing coleadership of programs.
- Consensus partnership decision making.
- Communicating genuine interest in stakeholder input (e.g., via codrafting).

- Adequate engagement from federal agencies beyond DHS.
- Government follow-through on partnership-related decisions.
- Adequate and competent support services.

Examples of Use of These Best Practices

We conclude with two examples of partnership programs, the development of the NIST Cybersecurity Framework and the CSRIC Working Group 4 program conducted by the FCC and the Telecommunications Sector Coordinating Council.

Both programs follow most if not all of the best practices identified in the previous study and were publically judged to be successful by both industry and government.

Collaborative Framework Development Proposal

INTRODUCTION

The NIST Cybersecurity Framework was designed as a voluntary collaborative industry-government effort pursuant to Executive Order 13636. The Framework enjoys broad support both in industry and government and the incoming Administration and Congress should continue to use the voluntary Framework as the basis for cybersecurity efforts.

Now, essentially three years since the Framework was developed, some are seeking clarification as to its usefulness and effectiveness. These questions are legitimate. However any program that seeks to provide data on these topics must remain consistent with the voluntary and collaborative nature of the Framework's development and implementation. The Framework cannot be mutated into a regulatory model without serious negative impacts on our nation's security and the partnership process that gave birth to the Framework.

Fortunately, the partnership process as outlined in the National Infrastructure Protection Plan (NIPP) can be used to design sector specific programs that may be able to provide information useful for further policy development consistent with the voluntary collaborative model. Executive Order 13636 they called for the Framework to be deployed in a prioritized, and cost effective manner and for the government to design incentive programs to promote voluntary use of the Framework. The proposal outlined below will enable these as yet not fully realized aspects of Framework deployment to be realized without violating the fundamental precepts upon which it was created.

USING THE PARTNERSHIP PROCESS IN THE NIPP TO EVOLVE THE NIST FRAMEWORK

THE NIPP calls for each critical industry sector to have a Sector Coordinating Council (SCC) and a sibling Government Coordinating (GCC) Council. Each sector's GCC and SCC should be tasked with collaboratively designing an appropriate assessment plan for the Framework's use within that specific sector.

It is absolutely critical that there be a mutual understanding and commitment to the collaborative process and that both the GCC and the SCC understand what is meant by the term "collaborative process"

Fortunately, the Department of Homeland Security, in conjunction with the IT SCC have conducted research published in the winter 2015 edition of the refereed Journal of Strategic Security that defines the practices that create successful partnership programs for cybersecurity. The Partnership For Critical Infrastructure Security has endorsed this list of best practices, which is the private sector entity, which coordinates security issues for the designated critical industry sectors. The GCCs and SCCs should commit to following these practices in running the assessments program outlined below.

In summary these best practices are:

- Senior-level commitment to the partnership process, as defined below, communicated to participating organizations' staff and upper echelons.
- Mutual and equal involvement of both industry and government at the priority, goal, and objective phases of projects, not just implementation.
- Reaching out to stakeholders early on, ideally at the "blank page" stage.
- Continuous and regular interaction between government and industry stakeholders.
- Providing adequate time for stakeholder review (equivalent to government review).
- Establishing co leadership of programs.
- Consensus partnership decision-making.
- Communicating genuine interest in stakeholder input (via codrafting).
- Adequate engagement from associated government agencies to avoid duplication
- Government follow-through on partnership-related decisions.
- Adequate and competent support services.

HOW TO DESIGN THE FRAMEWORK ASSESSMENT PROCESS

These designs should determine:

- What would "count" as "adoption" of the Framework suitable, which, in turn, would be suitable for eligibility of access to a menu of incentives.
- What aspects of the Framework are cost-effective for deployment.
- Other goals as determined jointly by the SCCs in conjunction with the GCCs for each sector.

Since each critical sector has unique characteristics the specific design of the process needs to be tailored to the unique characteristics of that sector. It must also be appreciated that organizations within a sector will have unique characteristics and hence the voluntary nature of use of the Framework must be maintained. Because of this the sector assessments can only be used to develop broad themes and not requirements applicable to all within the sector. That being said industry wide research of this nature can and often does generate useful information that can be applied on a voluntary basis for groupings within a category that do share common issues and restrictions.

With this precept in mind we would anticipate the joint SCC/GCC entities would:

- Seek out private sector organizations that are generally representative of the target audience for which the Framework is intended for use as envisioned in Executive Order 13636.
- Solicit the voluntary, and anonymous participation of those organizations in the assessment procedure.
- Identify the government agency that will provide the "install," educate the critical infrastructure end-user on the Framework intent and purpose, provide the knowledge and training on how to implement the Framework in a manner agreed to as appropriate for that organization and provide assistance to the end-user in:
    - Identifying the "golden nuggets" to be protected;
    - Selecting the right maturity level (tiring) for its organization;
    - Developing a sustainment plan.
- Engage the GCC or sector specific agency to assist any entity that volunteered in deploying the Framework and jointly set appropriate goals and metrics. Possible metrics could include:
    - Measurements of "effort required";
    - Measurements of time to implement/maintain;
    - Measurements of cost to implement (people/equipment) and maintain;
    - Assessment of meeting the agreed to outcomes;
    - Determination to the best degree possible of the cost effectiveness of the use of the Framework
    - Determination of what, if any, elements of the Framework were effective, but not economically sustainable
    - Assess what market incentives (not regulatory mandates) might be provided to future organizations within the sector that would make effective, but uneconomically sustainable, elements of the Framework economically reasonable for voluntary adoption
    - Identify any unanticipated or anticipated, deployment problems and make recommendations back to the partnership as to appropriate next steps such as streamlined process or needed additional incentives.

Under this proposal, it is assumed that participating critical infrastructure entities will be donating internal resources to this effort (which will be accounted for in the costs column) and government will be contributing resources to assist with deployment, provide for the assessments and ensure the vision of the Framework is properly captured.

Data from the tests would be anonymized so that no specific data related to any private sector entity would be made available. There should be no requirement that any participating entity publically acknowledge either its participation or the results of any testing.

This proposal would be an organized, scientific process that utilizes the existing official partnership structure to systematically and independently determine key elements of the Framework, which are not achievable or otherwise cost-effective under the current government plans.

Appendix A – Detailed Incentives

Among the benefits of the above program is that it should identify uses of the Framework that are cost effective within specified classes of critical infrastructure entities. Such finding ought to provide a significant stimulus for voluntary adoption of the Framework, as companies will naturally adopt measures that are shown to be cost effective.

The program will likely also identify uses of the framework that may be effective from a security perspective, but are not cost effective. These too are important findings as in an interconnected world major elements of critical infrastructure may lie in private hands and the particular private entities may not be able to sustainably secure them particularly against sophisticated attacks such as by nation states.

In these cases government has already recognized via the House GOP Task Force Report on Cybersecurity and President Obama's EO 13636, that a menu of incentives needs to be deployed. Unfortunately, apart from the recently enacted information sharing legislation that uses liability incentives to promote information sharing, little additional work has been done in this area.

This appendix provides outline potential incentives that could be adapted by the SCCs and GCCs as appropriate to the specific sector studied. Some of these incentives are outlined below with more extensive explanations to follow.

- Process Preference – The government could use Framework "adoption"/test participation as criteria for prioritizing applications to obtain the following:
    - SAFETY Act designations and certifications;
    - Patent approval;
    - Security clearance;
    - Permitting and/or other governmental approvals.
- Modification of the SAFETY Act to better encompass cybersecurity.
- Streamlined Compliance – The government could map the Framework to existing compliance regimes and allow participating test entities to use it as a tool to "audit once, report out to various regulators many times."
- Procurement Advantaging:
    - A federal acquisition incentive could include relief from certain other Federal Acquisition Regulation requirements that are overly burdensome and not germane for the supplied product or service if an entity adopts the Framework;
    - Include indemnification or partial indemnification for claims arising from supplied products.
    - Federal acquisition preferences, such as those already offered to minority-owned business, woman-owned small business, and veteran-owned small business programs as described in The Veterans Benefit Act of 2003; Small Business: 15 USC 633 et seq; Women and Minorities: 15 USC 637; the Office of Federal Procurement Policy Act of 1974 (Pub. L. 93-400);
    - Federal acquisition rebates as utilized in the "Indian Incentive Program" – http://www.acq.osd.mil/osbp/sb/programs/iip/

- Brand Recognition.
- Technical Assistance.

1. **Streamlining Regulation and Reducing Audits:**

To the extent that is possible, the federal government should streamline redundant regulations where they exist, allowing private sector entities to better allocate resources toward improving the security of their organization, and by consequence, the nation's. Specifically, the government might map the NIST Cybersecurity Framework to existing compliance regimes and allow companies that participate in the test process to use it as a tool to "audit once, report out to various regulators many times." ISA as well as several other prominent trade groups, including the Business Software Alliance, US Chamber of Commerce, TechAmerica, and Center for Democracy and Technology, have advocated for years the need for regulatory streamlining which would save time and resources for both the private and public sectors.[1]

In a recent statement, a large US bank indicated that requests from a multitude of regulators have increasingly become redundant. The bank continually receives the same requests from different regulators which has resulted in a 500 percent increase in the amount of resources spent synthesizing customized, but largely identical reports to accommodate these redundant requests.

A system of regulatory mandates applied to the broad and diverse private sector is not effective, and is actually counter-productive, in generating substantial improvements in private sector cybersecurity from both a national economic, as well as a national security perspective.

Recently, a large US defense contractor reported an annual decrease in the amount of penetration testing and security monitoring the organization conducts because the organization had to reallocate the staff, time, and resources previously spent on security to respond to regulatory requests and audits.

The regulatory agency model of governance was created during the 19th century to address the hot technology of that day—the railroads. And, while rail travel today is remarkably similar to what it was in the 1800s, the Internet is characterized by nearly daily change. The process of developing effective regulations is inherently time consuming. There is virtually unanimous agreement that any regulations specific enough to assure improved security quickly become outdated soon after their enactment.

2. **Federal Grants & Tax incentives:**

The federal government could provide additional grant funding and tax incentives that encourage establishing additional cybersecurity investments. Grant funding has been used effectively in other homeland security areas such as emergency preparedness and response and should be further utilized

[1] http://isalliance.org/publications/2C.%20Industry-Civil%20Liberties%20Community%20Cybersecurity%20White%20Paper%20-%20Improving%20our%20Nation's%20Cybersecurity%20through%20the%20Public-Private%20Partnership%20-%203-2011.pdf

and promoted. Critical infrastructure industries can use grant funds for research and development, to purchase equipment, and to train personnel necessary for the adoption of cybersecurity best practices such as the NIST Framework. Again, this approach for providing grants and tax incentives has been widely endorsed by industry for years as evidenced in ISA's trade association white paper on the public-private partnership.[2]

While tax incentives are often politically contentious, this approach may be targeted to smaller and medium-sized businesses. SMEs are a weak link in the cybersecurity supply chain and, without incentives, they may never perceive compliance with effective cybersecurity practices to be economically beneficial.

These grants and tax credits would allow these smaller private sector entities to adopt or develop the best practices included in the NIST Framework that might be very effective for increasing their cybersecurity within their business or sector, but might be less cost effective.

These tax incentives and federal grants could be made available to small to medium organizations who participate in a sector-by-sector test of the NIST Framework to identify which elements of the Framework are most beneficial and/or cost effective.

One of the benefits of this approach is that there is no significant impact on the federal budget due to the fact that this money is already designated for distribution. Furthermore, there is the potential for relatively immediate impact since existing standards, best practices, and government programs can be utilized and adapted to future needs since most applications must be periodically renewed. Finally, a renewal process in place for these types of government contracts will allow for compliance testing as a means of approving and of continuing the contracts. The reach of the positive effect of this approach will go beyond major players to include a broader universe of suppliers and contractors to CI/KR

3. Fast-Track Patent Pilot to Promote R&D

Research and development efforts at critical infrastructure companies are susceptible to the ongoing threat of trade secret theft from rouge cyber criminals and state-sponsored entities. The Patent and Trademark Office should explore building a fast-track patent pilot for private sector organizations that voluntarily adopt the best practices outlines in the NIST Framework. This could provide a significant incentive for R&D-intensive critical infrastructure companies to adopt or otherwise use the Framework. This market incentive for adoption of voluntary best practices was specifically highlighted by the Department of Commerce in its incentives report to the President pursuant of Executive Order 13636.[3]

4. SAFETY Act Designations

Congress could update the SAFETY Act to better appreciate the cyber threat that has become more evident since its enactment. The act, which provides a mix of marketing, insurance and liability benefits for technologies designated or certified by DHS, can be expanded to standards and best practices, such

[2] Ibid

[3] http://www.ntia.doc.gov/files/ntia/Commerce_Incentives_Recommendations_Final.pdf

as those found in the NIST Framework, as well as technologies that protect against commercial as well as terrorist threats.

By designating or certifying organizations under the SAFETY Act for developing or using cybersecurity technology, best practices, and standards, these organizations can similarly take advantage of marketing and insurance benefits, which can provide tangible business paybacks and encourage cybersecurity spending beyond what was justified by their initial business plans. The program has proven successful in the physical arena and should be reexamined to apply to cyber.

5. Leveraging Procurement Policy and Purchasing Power of Federal Government

Government could increase the value of security in the contracts it awards to the private sector, thereby encouraging broader inclusion of the level of security provided to government. In turn, this would facilitate broad improvement of the cybersecurity posture among critical infrastructure owners and operators. The result of "building in" effective cybersecurity in products and services that are developed and delivered to the government at inception will not only insure the public's best interest but if such requirements were extended to secondary suppliers and sub-contractors as well, this initiative could have a significant effect on down-stream entities.

Such modifications to procurement policy might include:

- A federal acquisition incentive could include relief from certain other FAR regulations that might be overly burdensome and not germane for the supplied product or service if an entity adopts the Framework.
- Include indemnification or partial indemnification for claims arising from supplied products.
- Federal acquisition preferences, such as those utilized in the minority-owned business, woman-owned small business, and veteran-owned small business programs as described in The Veterans Benefit Act of 2003; Small Business: 15 USC 633 et seq; Women and Minorities: 15 USC 637; the Office of Federal Procurement Policy Act of 1974 (Pub. L. 93-400).

While this approach does have the potential for substantial benefits, government would need to enhance the value of its contracts because a number of the smaller organizations within the supply chain do not have the same massive incentive to adopt government specifications that some larger players do. While this approach has potential for real and immediate benefits, it is important that government realize that such compliance cannot be expected to come "for free." National security has a cost, and that cost is the government's responsibility.