INTERNET SECURITY ALLIANCE
www.isalliance.org

Senate Commerce Committee Memo on Presidential Executive Order

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

The Internet Security Alliance (ISA) supports President Trump's new executive order on cybersecurity, and looks forward to assisting in its implementation. The Senate Committee on Commerce, Science, and Transportation, with its jurisdiction covering interstate commerce, has broad authority over key elements of the Order. ISA suggests the Committee consider some of the following recommendations as it exercises its oversight function of multiple critical infrastructure sectors.

BACKGROUND: WHAT IS CYBERSECURITY RISK MANAGEMENT?

The essence of the President's order places responsibility for cybersecurity on Agency heads that are to use a risk management model in conducting cybersecurity programs. ISA supports this critical paradigm shift.

As Government Accountability Office (GAO) testimony has pointed out, federal systems traditionally have not used the risk-management model for cybersecurity, opting instead for a "policy model" in which agencies check off whether they have complied with a set of standards or requirements (i.e., policies).[1] Under a risk management model, more commonly used in the private sector, a forward-looking analysis of threats and critical vulnerabilities determine what issues the organization is likely to face. Security practice is then implemented based on this forward-looking risk analysis.

Independent research has shown that the private sector risk management model is preferable to the policy model traditionally used in the government.[2] Generally, federal systems perform poorly and often rank last in comparison on critical items, such as fixing security problems in software they build and buy.[3]

A critical element of cybersecurity risk management is that scarce security resources are focused on areas in most need of attention and where they are most beneficial. Again, historically, federal efforts have not generally followed this precept of risk management. For example, federal spending tends to focus on purchasing IT equipment without considering the personnel training required to use that equipment effectively. Large providers, who generally do comparatively well with cybersecurity, are the central focus of federal efforts, rather than the smaller players interconnected to the system, where risks are greater. These efforts also fail to include cost-benefit feedback loops, which are needed to develop metrics for effectiveness and cost-effectiveness to guide future policy decisions.

Additionally, the Committee should be mindful of the findings of the National Infrastructure Protection Plan (NIPP), which observes the private and public sectors assess cyber-risk differently and adds another complicated layer to the cybersecurity calculus for the private sector, which operates under a mandate to maximize shareholder value.[4]

2500 Wilson Boulevard #245, Arlington, VA 22201-3834, United States of America | (t) 703 / 907-7090 (f) 703 / 907-7093

This reality generates a higher level of security risk tolerance in the private sector than the public sector. For example, a private entity may be comfortable with allowing 10 percent of inventory to "walk out the back door" every month because it will cost 11 percent to purchase the additional guards and cameras to fully secure themselves. The public sector does not have this luxury – government has enormous non-economic concerns it must accommodate, such as national security and privacy.

Government must realize the aligned, but not identical, needs of the public and private sectors, and devise a sustainably secure system that maximizes scarce resources while allowing for necessary capital to flow throughout the economy.

ISA would like to offer five specific recommendations the Committee should consider as it exercises its oversight functions of the President's order.

SUMMARY OF RECOMMENDATIONS FOR CREATING A SUSTAINABLY SECURE CYBER SYSTEM

The following recommendations ought to be considered when discussing steps to meet the challenges of the Digital Age:

1. Cybersecurity programs need to be rebalanced to better address the broad strategic and economic obstacles to cyber-risk management, not merely the technical issues.
2. Agency heads should receive cyber-risk management training, modeled on the successful handbook developed for the National Association of Corporate Directors.[5]
3. Improve transparency in government information sharing efforts and establish norms for incident reporting and information sharing.
4. Encourage and broaden public-private collaboration, and emphasize improved cybersecurity of small- and medium-sized businesses, third parties through which cyber-attacks are launched.
5. Workforce Development: Awareness yields to understanding and makes cybersecurity cool.

RECOMMENDATIONS

1. Cybersecurity programs need to be rebalanced to better address the broad strategic and economic obstacles to cyber-risk management, not merely the technical issues.

Section 2(b)(i) and (ii) of the Order calls on the Secretary of Homeland Security to "identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities identified pursuant to section 9 of Executive Order 13636" and to "evaluate whether and how the authorities and capabilities identified…might be employed to support risk management efforts and any obstacles to doing so."

Virtually all commentators, from government and industry, agree we are currently losing the fight with the cyber-attack community. ISA believes a major reason is because we have not been addressing the main obstacles to creating a sustainably secure cyber system.

2500 Wilson Boulevard #245, Arlington, VA 22201-3834, United States of America | (t) 703 / 907-7090 (f) 703 / 907-7093

A series of independent research studies, including by PricewaterhouseCoopers (PwC)/CSO magazine and McAfee/CSIS, have all shown that the largest obstacles in promoting cybersecurity for critical infrastructure are economic.[6] The reality is, virtually all the economic advantages favor the attacker.[7] Recent evolution of cyber-attack methods also increase the threats on these structures.

Cyberattacks are comparatively cheap and easy to access. They generate enormous profits—$500 billion to $1 trillion by 2018—and there is very little effective law enforcement.[8] We successfully prosecute perhaps 1 to 2 percent of cyber attackers while the attack community, fueled by their enormous profits and in many cases state sponsorship, is becoming increasingly sophisticated.[9]

While critical infrastructures, such as the power grid, have been technologically vulnerable to attack from cyber-crime syndicates for some time, we have not seen the attacks materialize due to international economic interdependence of nation-states, likely retaliation, and limited economic incentive to attack such critical infrastructures. But, with the explosion of ransomware attacks, the economic incentives shift, providing more financial opportunities for cyber criminals to attack critical infrastructures, such as the telecommunications and utilities sectors. Just as hospitals have been held hostage to cyber ransoms, utilities may be in the future, potentially for much larger amounts.

Cyber defenders need to protect an inherently insecure system that is becoming increasingly vulnerable. Due to the massive interconnection that is endemic to the Internet, no entity—including government—can account completely for its own security. While large core infrastructure providers do generally well with cyber defense, they are interconnected with innumerable smaller players who often lack the economies of scope and scale required to effectively protect their systems. These smaller players are the soft under-bellies of cyber defense that would be prioritized in a true risk management analysis.

PwC, in its 2016 Global Information Security Survey, found that nation-states and well-resources criminal organizations are beginning to collaborate on cyber-attacks, routinely assessing target defenses, and designing new methods to circumvent existing defenses.[10] This creates a potential resource imbalance even for the largest of critical infrastructure organizations. It is unreasonable to expect private institutions to fight off cyberattacks from entities who dwarf them in size and scope. For a level of security necessary for national security, but not reasonable for private organizations to provide on a sustainable basis, a new dynamic system of market incentives is needed.

The Committee should embrace the directives in Executive Order 13636, which created the NIST Cybersecurity Framework and called for the establishment of a set of incentives to promote private sector cybersecurity.[11] The House GOP Task Force of Cybersecurity's top recommendation was also to create a menu of incentives for the private sector to address the economic imbalances of the digital age. Yet, there has been very little work in this area.[12]

Industry must lead in developing cost-effective measures for addressing cyber resilience and take appropriate steps – both technically and organizationally – to manage risk. Flexibility is important as solutions may differ depending on the nature of organizations, services, and markets.

2500 Wilson Boulevard #245, Arlington, VA 22201-3834, United States of America | (t) 703 / 907-7090 (f) 703 / 907-7093

Ironically, federal policy routinely provides for market incentives in multiple areas of the economy, including environment, agriculture, pharmaceuticals, defense and even security (e.g. the SAFETY Act). Given the centrality of cyber economics to addressing this issue in a risk management format, the Committee ought to use its tools and processes available to coordinate and assist agencies in developing a set of market incentives to promote national cybersecurity. As the House GOP Cybersecurity Task Force noted, a menu of incentives may be required as different incentives will be applicable to different industry sectors with good actor incentives, such as permitting, patenting, procurement, with tax credits and grants targeted for smaller players in critical infrastructure supply chains.[13]

2. Agency heads should receive cyber-risk management training, modeled on the successful handbook developed for the National Association of Corporate Directors[14]

Section 1(a) of the Order states, "The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises [and] …it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise**."** The Order further states, "cybersecurity risk management comprises the full range of activities undertaken to identify and protect IT and data…" and that "effective risk management requires…integrated teams of senior executives with expertise in IT, security, budgeting, acquisition, law, privacy, and human resources."

ISA believes that the elevation of cyber-risk management to agency heads is a major step in the right direction and very consistent with the trend that has taken place over the past several years within leading private sector organizations. It is imperative that critical infrastructures shift focus from cybersecurity compliance to cybersecurity risk reduction. Cyber experts who are diverted to address regulatory compliance must refocus attention to actual security measures to protect their institutions and build trust within the sectors.

However, are federal agency heads necessarily sophisticated in the cybersecurity field to manage these programs? Probably not. Agency heads at federal, state and local levels are selected due to their subject matter expertise, which in most cases does not include understanding the subtleties of cyber-risk management. Indeed, most Agency heads, like corporate directors, are "digital immigrants" who were not born into the digital world they now inhabit. Moreover, like corporate directors, Agency heads tend to be focused on the broad strategic issues affecting their organizations and are burdened with demanding schedules. This lack of cybersecurity knowledge and understanding could be a prime obstacle to Agency heads effectively addressing security challenges.

To address these issues in the private sector, the National Association of Corporate Directors (NACD) developed a Cyber-Risk Oversight Handbook and training program that views cybersecurity issues not in their purely technical sense, but by embracing a full range of organizational strategic aspects.[15] The NACD program must not be confused with other ongoing training programs that focus solely on how to secure and protect passwords, emails, and mobile devices. Rather, the NACD program has proven

2500 Wilson Boulevard #245, Arlington, VA 22201-3834, United States of America | (t) 703 / 907-7090 (f) 703 / 907-7093

results in positively changing the way corporate boards address cybersecurity issues and approach cyber-risk management.

In its 2016 Global Information Security Survey, PwC found use the NACD Handbook results in greater commitment to cybersecurity on an enterprise-wide basis, better cyber-risk management, better alignment of cyber with overall organizational goals, better communication about cyber-risk throughout the organization, and creating a culture of security for the enterprise.[16]

Agency heads are the government equivalent of corporate board members and ought to receive the similar training to what leading corporate boards receive to manage cyber risk effectively within their organizations.

The Committee, using its various resources and tools, should assure all agency heads, not just the IT departments, and lower level staff receive adequate cyber-risk management training, modeled on the successful NACD program. This training should cover the full range of activities involved in cyber-risk management. Just as corporate boards have recognized their subject matter expertise does not necessarily prepare them to effectively manage cybersecurity risk and are getting training to overcome this obstacle, so too ought federal Agency heads. Absent this training, it is unlikely that the Agency heads in all cases will be prepared to fully implement risk management frameworks.

3. Improve transparency in government information sharing efforts and establish norms for incident reporting and information sharing.

Any assessment of the readiness of the United States to manage the consequences of a cyberattack must come to grips with the state of information sharing between the public and private sectors.

Sectors of critical infrastructure have a long history of collaborating with government. However, the sectors require a better understanding of how the government and the national security apparatus use the information they supply, and what protections will be put in place to keep sensitive data confidential.

These issues will need to be addressed to foster sound public-private partnerships and a fundamental relationship of trust and collaboration between the private-sector stakeholders responsible for delivering our nation's electricity and the government.

Greater transparency will not only increase the volume of communication, but also improve the quality of information exchanged to assist in government-led investigations. In the past, some critical infrastructure sectors have been reluctant to share certain data with the government due to privacy concerns. Many utilities have noted that they will only be comfortable sharing more detailed information on cyber intrusions if they know, understand, and trust the processes the government uses to protect it.

2500 Wilson Boulevard #245, Arlington, VA 22201-3834, United States of America | (t) 703 / 907-7090 (f) 703 / 907-7093

Separately, it is in the business interest of industry to appropriately share information on cyber incidents with their customers. In the face of an attack, it is better to be upfront than attempt to hide system or data compromises. Being less than frank is redolent of conspiracy and once the facts inevitably become public, the focus changes from how the sector entity was victimized to how it hid the truth. However, certain disclosures may be seen by the law-enforcement community as compromising ongoing investigations. As a result, the problem of norms around sharing information must be addressed in order to find suitable middle ground toward the goal of better alignment with business imperatives.

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 audits) should not be allowed to disrupt or undermine industry attempts to mount an appropriate and proportionate response. Furthermore, incident notification should account for disruptive effects in adjacent sectors and obligations on other parties to share relevant information in a timely manner. Cooperation and information sharing should be voluntary and protected, and the law should favor incentives above regulations.

The Committee, using its various tools and processes, could highlight these obstacles to cyber-risk management and suggest concrete steps to improve this process throughout the government.

4. Encourage and broaden public-private collaboration, and emphasize improved cybersecurity of small- and medium-sized businesses, third parties through which cyber-attacks are launched.

The President's Order wisely observes that, as part of the cyber-risk management process, agencies will be "held accountable by the President for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes." As government agencies operationalize the broad cyber-risk management process called for in the President's Order, they will almost inevitably need to collaborate with the private sector.

The Committee should be mindful of the findings of the National Infrastructure Protection Plan (NIPP), which noted that due to the fact the vast majority of cyber infrastructure, including that which the government uses, is owned and operated by the private sector, managing cyber-risk needs to be done through a public-private partnership. [17] Moreover, as mentioned above, the NIPP observes that the private and the public sectors assess cyber risk on very different dimensions. The private sector operates under a mandate to maximize shareholder value, transforming cybersecurity into an almost entirely economic endeavor, whereas the public sector has enormous non-economic concerns, such as national security and citizen privacy. This reality generates a higher level of security risk tolerance in the private sector than the public sector.

Among the most important findings of ISA's work in *The Cybersecurity Social Contract* is that the government has effectively evolved a two-tiered system for cybersecurity information sharing. [18] In the first tier are large businesses that have developed systems more resilient to cyber-attacks. In the

2500 Wilson Boulevard #245, Arlington, VA 22201-3834, United States of America | (t) 703 / 907-7090 (f) 703 / 907-7093

second, critical supply chain participants – an ecosystem of smaller, less capable companies – who have substantially less effective systems and who are effectively left out.

In addition, new regulations in the Federal Acquisition Regulation have significantly increased costs of doing business with the government and shifted the focus away from risk management to compliance with standards. These increased costs dwarf information technology budgets for small businesses while not adding measurably to enhanced security. In fact, this "policy model," typically practiced by federal agencies, has been shown less effective from a security perspective than the more forward-looking risk management models that are less dependent on traditional standards compliance.

Smaller companies are more vulnerable than larger ones, understand the issue less, are investing less, and are the segment that most in need of government help. Government should restructure its programs to make them more user-friendly to smaller firms. In addition to simply sharing the technical information, government, working collaboratively with larger enterprises, needs to place a higher priority on making this information actionable. This generally means simplifying it or making it "passive." As federal agencies assess their authorities and capabilities, we urge them to develop a plan for trusted and reliable automated information sharing, targeted to the small business community.

Solving this requires a dialogue between critical infrastructure sectors, vendors, and the government to evaluate possible solutions that cost-effectively increase confidence in U.S. cyber resiliency.

The Committee, using its various tools and processes, could highlight these obstacles to cyber-risk management and suggest concrete steps to improve this process throughout the government.

5. Workforce Development: Awareness yields to understanding and makes cybersecurity cool.

Section 3(d)(i)(A) states that the secretaries of Commerce and Homeland Security, in consultation with the secretaries of Defense, Labor, Education, and the Office of Personnel Management director, must "jointly assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education" and provide recommendations on "how to support the growth and sustainment of the nation's cybersecurity workforce in both the public and private sectors."

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 we just cannot fill. The worst part, this deficit is expected to continue for some time.

Standard management best practice is to begin an initiative with clear goals. To address cybersecurity workforce gaps, we need to focus on recruiting people to help fill the void, which like the issue itself, goes beyond technical expertise and runs to overall risk management. We need an integrated,

2500 Wilson Boulevard #245, Arlington, VA 22201-3834, United States of America | (t) 703 / 907-7090 (f) 703 / 907-7093

multifaceted, targeted program with research-based messaging, just as the private sector would do when marketing any product or service.

From primary education, we need to reach kids where they are and integrate cybersecurity into what they 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 towards, potentially creating a pathway to reach tech-interested youths, complimented by camps and contests where the seed of developing a career doing what they love could be planted.

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 to secure the ecosystem as opposed to a particular company. Government's primary mission ought to be to coordinate with the private sector on these programs, rather than devising their own independent programs. Government can open doors, facilitate partnerships, and allow the private sector to be the major creators and operators of workforce-development programs.

The military provides another model for developing this cross-sector collaboration. The 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. Programs such as Cyber Guard, operated by the Software Engineering Institute at Carnegie Mellon, utilize online capabilities to deliver effective exercise training to support these efforts across the country. This training model is now also being utilized by the civilian workforce as well.

ISA's *The Cybersecurity Social Contract*, referenced earlier, includes several additional recommendations for building an effective national cyber workforce strategy. We would be happy to assist the Committee by providing further detailed recommendations or meeting with the Committee staff to discuss.

In conclusion, the Internet security Alliance believes President Trump has opened up an unprecedented avenue for vastly improved cybersecurity. The House Energy & Commerce Committee has the opportunity to reshape the policies that have failed to improve the cybersecurity posture of the nation while exacting considerable costs. Please let us know how we can assist you further in this very important task.

Sincerely,

Larry Clinton

Larry Clinton

2500 Wilson Boulevard #245, Arlington, VA 22201-3834, United States of America | (t) 703 / 907-7090 (f) 703 / 907-7093

President/CEO
Internet Security Alliance

[1] ***Enhancing Cybersecurity of Third-Party Contractors and Vendors***, 114th Cong. (2015) (testimony of Gregory C. Wilshusen, director of Information Security Issues, US Government Accountability Office), Web.
[2] Veracode, ***State of Software Security Report, Volume 6: Focus on Industry Verticals*** (Veracode, June 2015), Web.
[3] Ibid.
[4] "National Infrastructure Protection Plan," Department of Homeland Security, 2013, Web, July 6, 2016.
[5] Larry Clinton, AIG, and NACD, ***Cyber-Risk Oversight: Director's Handbook Series*** (National Association of Corporate Directors, 2014), Web.
[6] PricewaterhouseCoopers. ***The Global State of Information Security*** PwC, 2008). Center for Strategic and International Studies and McAfee, ***Net Losses: Estimating the Global Cost of Cybercrime*** (Intel Security, June 2014), Web.
[7] Center for Strategic and International Studies and McAfee, ***Net Losses: Estimating the Global Cost of Cybercrime*** (Intel Security, June 2014), Web.
[8] Executive Office of the President of the United States, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," ***Whitehouse.gov,*** 2009, Web.
[9] Ibid.
[10] PricewaterhouseCoopers. ***The Global State of Information Security*** PwC, 2008). Center for Strategic and International Studies and McAfee, ***Net Losses: Estimating the Global Cost of Cybercrime*** (Intel Security, June 2014), Web.
[11] Exec. Order No. 13636, 3 C.F.R. Section 7(a)(2013), Web.
[12] US Cong. H., House Republican Cybersecurity Task Force, ***Recommendations of the House Republican Cybersecurity Task Force,*** 112th sess., H. Rep., Washington, DC, Oct. 2011, Web.
[13] Ibid.
[14] Larry Clinton, AIG, and NACD, ***Cyber-Risk Oversight: Director's Handbook Series*** (National Association of Corporate Directors, 2014), Web.
[15] Ibid.
[16] PricewaterhouseCoopers. ***The Global State of Information Security*** PwC, 2008). Center for Strategic and International Studies and McAfee, ***Net Losses: Estimating the Global Cost of Cybercrime*** (Intel Security, June 2014), Web.
[17] "National Infrastructure Protection Plan," Department of Homeland Security, 2013, Web, July 6, 2016.
[18] Larry Clinton, and David Perera, ***The Cybersecurity Social Contract: Implementing a Market-Based Model for Cybersecurity***, (Internet Security Alliance, Sept. 2016).

2500 Wilson Boulevard #245, Arlington, VA 22201-3834, United States of America | (t) 703 / 907-7090 (f) 703 / 907-7093