Collective Defense:
A Collaborative Perspective from the IT Sector

This paper is a collaborative effort based on the input and analysis from individuals in both the Information Technology (IT) Sector's Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) who participated in the Policy Leadership Working Group (PLWG). The objective of the PLWG for the purposes of this paper was to further define the concept of our Nation's "Collective Defense." This effort was co-chaired by Ms. Helen Jackson, Branch Chief, Partnership & Engagement, Stakeholder Engagement and Cyber Infrastructure Resilience Division, Office of Cybersecurity and Communications (CS&C), Department of Homeland Security (DHS) and IT GCC Chair, and Mr. Larry Clinton, President, Internet Security Alliance (ISA) who is a member of the IT SCC.

In addition to the support of the co-chairs, the paper was written and informed by the following participants:

IT GCC Participants

DHS
DHS Science and Technology Directorate (S&T)
DHS Office of Infrastructure Protection (IP)
General Services Administration (GSA)
Department of Justice (DOJ)

Industry Participants

Mr. Scott Algeier, IT-ISAC
Mr. Jeff Brown, Raytheon
Ms. Beverly Cenname, Northrop Grumman
Mr. Lou DeSorbo, Centene Corporation
Mr. Josh Higgins, ISA
Ms. Catherine Ide, Center for Audit Quality
Mr. Shaun McAdams, Raytheon
Mr. Gary McAlum, USAA
Mr. Coleman Mehta, Palo Alto Networks
Mr. Nasrin Rezai, General Electric
Ms. Ola Sage, E-Management
Mr. Carter Schoenberg, Hemisphere

Since this paper seeks to define the concept of "Collective Defense" with input from the IT SCC and GCC, many cybersecurity issues within the IT Sector and business community are explored, and some issues go beyond what the IT SCC and DHS have identified as immediate priorities for 2018 and beyond. The nature of the expanded scope of this paper, in part, focuses on some topics that are potential areas of future collaboration. While many topical issues within the information-security public policy and news landscape are only mentioned briefly, they are still of great importance to the IT Sector members.

Mission and Scope

Cybersecurity defenders across government and industry face a daunting but serious reality that self-defense alone can no longer be the governing practice. The need for a clearly defined *Collective Defense* apparatus, built upon the foundation of trust between industry and government, has become an issue of both national security and economic necessity. In addressing the IT SCC's 2018 Annual Meeting, DHS Under Secretary for National Protection and Programs, Christopher Krebs, shared a key economic difficulty in constructing this new model when he noted that private companies fund security at a commercial level appropriate to their needs, while government funds at a higher, national security level. To create a sustainable *Collective Defense,* we must find a way to fill this economic delta.

Anything less than a mutual, shared defense model cedes the advantage to our adversaries, which as noted by U.S. law enforcement agencies and the intelligence community, can be more organized than those within the defender community. In late 2017, the United States Government (USG) attributed the WannaCry cyber-attack to North Korea, and what followed was a collective call-to-action and an important expansion of the public-private partnership model that has defined our Nation's cybersecurity efforts to-date. DHS Assistant Secretary, Cybersecurity and Communications (CS&C), Jeanette Manfra, charged that "government and industry must work together now more than ever if we are serious about improving our collective defense. We cannot secure our homeland alone. A company can't single-handedly defend itself against a nation-state attacker."

WannaCry is just one recent example of the cyber-attacks of increased volume, velocity, and complexity that are targeting U.S. interests. The U.K. and U.S attributed Russian hackers for a campaign aimed at taking control of network devices (e.g., routers, switches) inside government, critical infrastructure and internet service providers, as well as also within small and home offices. Successful breaches of industry and governmental cyber defenses have led to unprecedented levels of unauthorized access to U.S. citizens' consumer data, as well as information of national security interest. These intrusions have seriously impacted corporate competitiveness, while undermining confidence in government stewardship. In constructing this new, more integrated *Collective Defense* model, it is crucial for everyone—industry, government, and the public— to be on the same side. We are being victimized by cyber-attacks, and unless we all work together to improve our current model of defense, the attackers will likely continue to win.

The Vision of the Department of Homeland Security's recently released Cybersecurity Strategy encourages a shared-responsibility model. The Vision states, "By 2023, the Department of Homeland Security will have improved national cybersecurity risk management by increasing security and resilience across government networks and critical infrastructure; decreasing illicit cyber activity; improving responses to cyber incidents; and fostering a more secure and reliable cyber ecosystem through a unified departmental approach, strong leadership, and close partnership with other federal and nonfederal entities."[1] This statement clearly recognizes strong leadership on the part of the federal

[1] Department of Homeland Security. 2018. "Cybersecurity Strategy." 1-35.

government is key to its goals of increasing security and resilience across government networks and critical infrastructure but acknowledges that the government cannot fulfill its stated goals alone.

Fortunately, multiple attempts to analyze and solve this problem by both industry and government have come to largely the same recommendations.[2] Creative mechanisms are needed to close the security gap while taking into consideration the issue of limited resources on both sides. Thus, the mission of this paper is to combine advanced technology with business economics and public policy to create a shared and sustainable cyber ecosystem that shifts the advantage to cyber defenders. Narrowing the security gap by leveraging the public-private partnership is key to developing a *Collective Defense* approach for our country.

The National Infrastructure Protection Plan (NIPP), which outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes, provides the following analysis: "Private sector organizations generally can increase their investments to meet their risk tolerances and provide for their community of stakeholders, but investments in security and resilience have legitimate limits. The government must provide for national security and operate with a different set of limits…Finding the appropriate value proposition among the partners requires understanding these differing perspectives…In a world in which reliance on critical infrastructure is shared by industry and government and where industry may be on the front lines of national defense, such as in a cyber-attack, a sustainable partnership must be developed to address both perspectives."[3]

Numerous examples of effective public-private partnerships in defending cyberspace exist, and the concept of partnering for defense is not new.[4] However, what has emerged since the time of these formative partnerships is the reality that there is a stark difference between the resources needed for commercial security and those needed for national security. This difference in resources is anecdotally

---

[2] House Republican Cybersecurity Task Force. 2011. "Recommendations of the House Republican Cybersecurity Task Force." Washington. The House Grand Old Party (GOP) report's primary recommendation was that Congress adopt a menu of voluntary incentives to encourage private companies' participation in improving cybersecurity. President Barack Obama's Executive Order (EO) 13636 "Improving Critical Infrastructure Cybersecurity" recognized the importance of incentives. It is noteworthy that neither of these two government reports – from differing political perspectives – advocated the use of traditional regulatory methods as "incentives." One of the noteworthy areas of consensus is that, due to the unique nature of the cybersecurity threat, including the speed at which technology and attack methods change, traditional regulation is a poor fit for addressing the problem. For a detailed analysis of how and why these traditional methods won't work in this space, see The Cybersecurity Social Contract (2016).

[3] Department of Homeland Security. 2013. "National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience." 15.

[4] For example, the IT-ISAC has been collaborating with the USG on operational and information sharing issues since before most modern sector-level infrastructure planning began. The USG has worked closely with its allies in industry to take common action through established groups such as the Cyber Threat Alliance. When the government attributed the 2017 WannaCry cyber-attacks to North Korea, industry organizations acted to disable a number of North Korean cyber exploits and disrupt their operations.

similar to the delta between the resources needed to fight street crime and organized crime. In both cases, a different level of coordinated and collaborative response is required. The defensive capabilities required to combat common cyber-criminals versus those vested with sophisticated, or nation state capacities is stark. Industry views the challenge similarly. The Pan-Industry Association white paper, "Improving Our Nation's Cybersecurity through the Public-Private Partnership" puts the issue in simpler terms.[5] This paper argues that the private sector should, and generally does, make investments to meet commercial security needs, consistent with their legal obligations to their shareholders, while it is the government's responsibility, under the Constitution, supported by taxes, to "provide for the common defense."

The following sections outline contributions made by both industry and government, with an inference toward which side will lead the effort, but the recommendations should not be read as unilateral assignments.

What Government Can Do

1. ***Continue to Promote Cybersecurity Efforts with Smaller Companies, Including Cost-Effective Use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework***

Small and medium-sized businesses (SMBs) represent more than 99% of all businesses in the U.S.[6] and are essential to our country's critical infrastructure and cybersecurity.[7] Many SMBs are vendors to larger companies and the USG. They are integrated into complex supply chains within the U.S. economy, and because of their importance, SMBs are often the target of cyber threats. SMBs that are part of the critical infrastructure supply chain are frequently at more of a disadvantage to cyberspace attackers than their larger counterparts, for a variety of reasons including limited budgets, access to timely, relevant and actionable information, technical expertise, and time to devote to comprehensive cybersecurity solutions. Given the importance of these SMBs to the Nation and their unique cybersecurity challenges, the government should pursue and sustain a collaborative process with industry and the SMB community to develop a comprehensive strategy to increase their overall cybersecurity.

The NIST Cybersecurity Framework enables organizations of all sizes to assess their cyber capabilities, understand and prioritize cybersecurity risks, and measure and track progress. While the NIST Cybersecurity Framework has been adopted by many large organizations,[8] many small and medium-sized businesses are still unaware of the Framework. Many SMBs that do attempt to use the NIST

[5] Pan-Industry Association. 2011. "Improving Our Nation's Cybersecurity through the Public-Private Partnership"
[6] SBA Office of Advocacy. 2017. "United States Small Business Profile" 1-4. https://www.sba.gov/sites/default/files/advocacy/United_States_1.pdf
[7] Symantec. 2017. "Internet Security Threat Report" 1-77.
[8] More information on the NIST Cybersecurity Framework, including on how small businesses can implement, is available at: https://www.nist.gov/blogs/taking-measure/framework-protecting-our-critical-infrastructure

Framework find that it could be more user-friendly and may not have the expertise to implement it, while others struggle with the expense involved in implementation. Fortunately, the market has responded and several commercial models have been developed (e.g., FAIR, X-Analytics)[9] that assist smaller entities in tailoring use of the Framework to their unique needs through prioritization and analyzing return on investment. As it moves forward with future iterations, the USG should work on measuring the NIST Framework's impact and cost effectiveness when it is adopted by an organization. The USG can also play a role, where possible and appropriate, in leveraging its experience to help identify best practices in cost-effective Framework implementation.

The Framework is an important piece in assisting our SMB partners, but there are also other ways government can play a role. The Small Business Administration (SBA) can also assist small companies by issuing loans, grants, or tax credits. SBA could explore requiring a percentage of the total value of these incentives to be allocated to cybersecurity and use of the Framework, if it makes sense given the IT assets of the business. For example, if an entity receives a SBA grant, loan or tax credit, the entity could be required to allocate a set percentage to the cybersecurity requirements or Framework usage. Further, a joint policy statement on the sharing of cybersecurity information from the Federal Trade Commission (FTC) and DOJ suggests that properly designed cyber threat information sharing is not likely to raise antitrust concerns. [10] This current guidance could be actively explored through a focus on collaborating with and supporting SMBs.

2. Prioritize and Operationalize Existing Recommendations and Best Practices to Address Commonplace Threats

While work remains to be done to establish our overall *Collective Defense*, much has been done by both industry and government to study how to address many existing pervasive cyber threats. Models for addressing these threats such as botnets and attacks on email security already exist.[11] This work puts the government in a unique position to act on these threats and create an economy of scale simply by making these models operational. The USG should build on these core guidelines by prioritizing them and identifying operational actions that can be taken to minimize these kinds of widespread threats and

[9] Factor Analysis of Information Risk Institute, Secure Systems Innovation Corporation, The British Standards Institution

[10]Federal Trade Commission, Department of Justice. 2014. "Antitrust Policy Statement on Sharing Cybersecurity Information" 1-9.

[11] The Trump Administration released EO 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. The report, "Enhancing the Resilience of the Internet and Communications Ecosystem against Botnets" released in response to EO 13800, establishes that effective tools exist to mitigate these threats but are not widely used. It also details a series of goals and corresponding actions that can be taken by government and industry to leverage these tools and minimize these threats. DHS's Binding Operational Directive 18-01 is another example of existing literature that details basic actions government and industry can take to protect themselves from email-based threats. The Administration should also leverage existing work on trusted online identities – such as the former National Strategy for Trusted Identities in Cyberspace – to improve baseline security against these types of attacks.

increase costs on cyber-attackers. This would also allow all involved parties to begin shifting focus away from low-level attacks to more systemic and complicated threats.

As one of the United States' closest allies, it is worth noting the United Kingdom's government model and vocabulary provided through its National Cyber Security Centre. Under the U.K. model, government and industry have focused on making cybercrime less profitable and riskier for malicious actors, by automating responses to "commodity" attacks and freeing up cyber personnel to focus on sophisticated threats.[12] "We wish to protect most of the people from most of the harm from most of the attacks most of the time," the UK cyber program's 2018 report states. The U.K. also uses the term "commodity" instead of "commonplace." The U.K. model could be a point of reference when the USG considers its own effective ways to combat cybercrime.

By prioritizing and operationalizing existing recommendations and best practices, the U.S. can address systemic risks in a sophisticated threat environment and boost the Nation's *Collective Defense*.

3. *Enhance Law Enforcement Cybersecurity Efforts*

Cybercrime (which research suggests costs up to $1 trillion annually)[13] has a tremendous impact on our shared cybersecurity. While the government's initial prioritization of national-level attention toward critical infrastructure protection was warranted to address existential risks, a substantially increased focus on other forms of cybercrime should now supplement those efforts. An important component of reducing cybercrime is increasing the deterrent effect of criminal prosecution. There is not much deterrence for cyber criminals and the lack of deterrence is made worse by the advent of nation-state supported criminal activity. Enhancing the partnership between the public and private sectors, within the law enforcement community is also a priority.

Coordination between law enforcement counterparts to facilitate investigations of data breaches and incidents needs to be further developed and a more efficient system for addressing cybercrime across international, federal, state, and local jurisdictions is needed. Industry also needs to work collaboratively with law enforcement (within the boundaries of individual companies' values) to the best extent possible to help law enforcement further its investigative capacity. Moreover, industry can assist law enforcement by reporting, and encouraging others to report, cyber incidents so law enforcement can use its resources to prevent and deter persistent cybercriminals. It is important to realize these efficiencies, because cybercrime investigations require speed to keep pace with criminal activity. The speed with which technology and cyber-attack methods change make it starkly different than other, more traditional forms of criminal activity.

The USG employs a "no wrong door" policy encouraging those who have suffered cyber incidents to report the incident to someone within the USG law enforcement community with whom they have a relationship as opposed to a specific entity. However, there is confusion on the part of industry about

[12] Levy, Ian. 2018. Active Cyber Defense - One Year On. UK National Cyber Security Centre.
[13] Clinton, Larry. 2016. The Cybersecurity Social Contract: Implementing a Market-Based Model for Cybersecurity. Internet Security Alliance 3-19.

who to report incidents to given varying levels of government interface. The government has attempted to reduce confusion through guidance documents and welcomes input from industry on how to more effectively disseminate and educate private sector communities about the resources available to them.[14][15]

Outreach to large and small businesses about these issues is important and should continue to ensure that companies who may be targeted for cybercrime are aware of how to contact their local federal law enforcement investigators and how law enforcement can assist them. Outreach efforts should not be exclusive to federal law enforcement and should include state law enforcement agencies and organizations such as the International Association of Chiefs of Police (IACP) to make these outreach efforts more robust. As law enforcement works towards this vision, government and industry can work together to improve industry's understanding of cybercrime threats; particularly for SMBs that lack the resources of larger companies. Cybercrime tabletop exercises help establish roles and responsibilities and include players at all governmental and industry levels. This cyber tool is a valuable resource, especially for stakeholder groups that may not interact as often with law enforcement.

To be clear, while increased coordination is needed at the highest national level, there have been examples of successful operational collaboration between law enforcement and industry that should be built upon.[16][17] Working partnerships like the Federal Bureau of Investigation's Cyber Task Forces, InfraGard, the U.S. Secret Service Electronic Crime Task Forces, and the National Cyber-Forensics & Training Alliance exist and demonstrate valuable information on a productive collaborative process. Law enforcement has dedicated resources to improving outreach to the private sector to identify opportunities for cooperation and bilateral information exchange.[18]

To enable more efficient law enforcement engagement across federal, state, and local agencies, new capabilities should also be developed to facilitate and expedite response and recovery capacity through collaboration with the insurance sector and enhance strategic law enforcement relations with international partners. Steps such as these can help our hardworking law enforcement officials more nimbly pursue cybercriminals. Government and industry agree that there is a need to increase the capacity of and training for law enforcement personnel across the country to correspond to the extent of the growing cybercrime threat. To further industry and law enforcement capabilities, efforts can focus on increasing coordination, developing and updating best practices, promoting the use of cyber

[14] Department of Justice. 2015. "Best Practices for Victim Response and Reporting of Cyber Incidents"
[15] United States Government. 2016. "A Unified Message for Reporting to the Federal Government"
[16] For instance, the multiple botnet takedown operations that law enforcement has conducted since 2011 were executed with the assistance of private sector computer security researchers, incident response firms, and Internet service providers.
[17] Moreover, the National Cyber-Forensic & Training Alliance has become an international model for uniting law enforcement, private industry, and academia to build and share resources, strategic information, and threat intelligence to identify and stop emerging cyber threats and mitigate existing ones.
[18] For instance, the FBI's 84 InfraGard chapters across the country provide the private sector with an opportunity to obtain technical data, cyber threat intelligence, and contextual information about cyber threats.

insurance, and communicating how to report cybercrimes and how to request law enforcement support. The private sector also believes that additional resources for law enforcement may be required.

4. Develop a System of "Good Actor" Incentives for Cybersecurity (Tailored to Industry Needs)

While the government believes that the market offers the most effective incentive for the private sector to adopt strong cybersecurity practices, government also recognizes that it must be willing to step-in to incentivize best practices when the marketplace alone proves insufficient to achieve national security levels of cybersecurity.[19] In the past, DHS has explored different ways to encourage improved cybersecurity practices by industry members and other entities while recognizing the importance of market-based incentives to promote positive change in organizations' business practices. As part of EO 13636, DHS evaluated numerous incentives in terms of their economic criteria, while remaining cognizant of feasibility in terms of costs and policy considerations.

Based on past evaluations, DHS remains committed to the following incentive concepts to encourage use of the Framework or other cybersecurity best practices as further defined by industry and government.

- **Regulatory Streamlining:** Research undertaken by the USG found that existing regulatory requirements, when complemented with strong voluntary partnerships, are capable of mitigating cyber risk to critical systems and information.[20] With support of its industry partners, the USG is open to identifying federal regulations that are excessively burdensome, conflicting, or ineffective.
- **Cybersecurity Research and Development**: DHS needs to continue its efforts with academia and relevant industry stakeholders to identify key priorities for research and development.
- **Procurement**: Every year, the USG makes significant investments in Information and Communications Technology (ICT). The Federal Government needs to ensure all of the products it buys are aligned to collective cybersecurity goals.

Industry holds the perspective that while these three incentives have been the focus of consideration for DHS in recent years, a renewed, broader, and more intensive analysis of the use of incentives to help fill the economic gap between commercial security and the national security is required for a *Collective Defense* model. The broader economy and U.S. history have plenty of examples of, non-regulatory market incentives, many of which are at a low cost to government and have promoted important outcomes that would have been challenging on a purely commercial basis. Incentive models in varying forms exist in many industries and sectors including: agriculture, aviation, pharmaceuticals, transportation, and even physical security. Industry requests the Federal Government's help to explore

[19] Daniel, Michael. 2015. The White House Blog: "Strengthening Cyber Risk Management" https://obamawhitehouse.archives.gov/blog/2015/02/02/strengthening-cyber-risk-management
[20] Daniel, Michael. 2014. The White House Blog: "Assessing Cybersecurity Regulations" https://obamawhitehouse.archives.gov/blog/2014/05/22/assessing-cybersecurity-regulations

other creative, non-regulatory, and cost-effective incentive concepts that may help close the gap between commercial and national security.

5. Streamline Cybersecurity-Related Regulations and Processes

One critical issue industry and government have in common is the scarcity of cybersecurity resources. Especially while facing a vastly expanding threat, it is critical that industry and government efficiently use their scarce resources. Much of critical infrastructure is already regulated, and often industry assumes and accounts for regulatory costs. However, cyber regulation is emerging in these sectors in an uncoordinated fashion with multiple jurisdictions crafting their own unique cybersecurity requirements.

Companies are having to comply with redundant requirements, which can divert scarce cybersecurity resources to duplicative tasks and thus, although well intentioned, undermine security. Some companies are reporting that 30–40 percent of their security budgets are being consumed by regulatory compliance.[21] Research is demonstrating that much of this regulation is in fact duplicative and, at times, in conflict.[22] Government can substantially increase the effectiveness of available cybersecurity resources by streamlining duplicative regulations to deconflict provisions between competing regulatory agencies. Analytical tools have emerged in the market that can assist in this effort to benefit all.[23] Government will also continue to engage with international counterparts to discuss proposed regulations that could harm international business and slow innovation.

6. Review, and Update as Needed, Strategies for National-Level Cyber Incident Response

Having an updated, and effective national policy for *Collective Defense* also requires an updated and effective national strategy for response and recovery. While organizations remain responsible for responding to attacks on their individual enterprises, there may be times when a cyber-attack has large-scale, national consequences that require a coordinated response from industry and government. Examples of such instances could include cyber-attacks that have physical consequences, cyber-attacks that result in supply chain disruptions, or cyber-attacks that result in prolonged outages of critical services or functions. While this is not an exclusive list of examples, the overall scale of cyber-attacks whose impacts extend broadly within a critical sector, or across multiple critical sectors or functions is beyond the ability of any one organization to adequately defend against, mitigate, or recover from the attack. An important category of these organizations is “ICT enablers,” the functions of whom are foundational to the cyber ecosystem, and often act in a fiduciary role to the ecosystem itself

[21] Clinton, Larry. 2016. The Cybersecurity Social Contract: Implementing a Market-Based Model for Cybersecurity. Internet Security Alliance.
[22] Feeney, Christopher. 2017. US Senate Committee on Homeland Security & Governmental Affairs: “Cybersecurity Regulation Harmonization”
[23] E.g. FAIR Institute, X-Analytics tools

and would likely be essential to assist with large-scale incident management, need to be identified respectively based on potential scenarios.[24]

The National Cyber Incident Response Plan (NCIRP) describes the national approach to dealing with cyber incidents and addresses, serving as an important foundation to, the important role the private sector, state and local governments, and multiple federal agencies play in responding to cyber incidents. However, the NCIRP is not a tactical or operational plan; rather, it serves as the primary strategic framework for stakeholders to understand how federal departments and agencies and other national-level partners provide resources to support response operations.[25]

Therefore, to ensure the Nation has a national cyber incident response strategy that can effectively address potential large scale, national level cyber incidents, it is recommended the government work with private sector organizations that have a responsibility for national level planning and coordination. The government can use sector coordinating councils through the Partnership for Critical Infrastructure Security (PCIS) and the Information Sharing Analysis Centers (ISACs), through the National Council of ISACs, along with other appropriate organizations, to review, and update as necessary, the current national policies for cyber incident response and recovery.

What Industry Can Do

1. Contribute to the Development of a National Common Operating Picture

There is widespread agreement that more enhanced sharing of threat information between government and industry is needed to prevent and rapidly respond to changing threats.[26] Assistant Secretary Manfra has stated a vision in which a cyber-threat only be used once.[27] Cyber threat information sharing is a tool that can help network defenders, within industry and government, identify, mitigate, and analyze current and emerging cyber threats. Information sharing helps develop a common operating picture.

Industry can enhance its contribution to the development of a common operating picture by increasing the amount of information sharing to trusted organizations and programs such as DHS' National

[24]National Security Telecommunications Advisory Committee. 2014. "Report to the President on Information and Communications Technology Mobilization" https://www.dhs.gov/sites/default/files/publications/ICTM%20Final%20Draft%20Report%2011-2014%20%282%29.pdf

[25] Department of Homeland Security. 2016. "National Cyber Incident Response Plan USCERT" https://www.us-cert.gov/ncirp

[26] House Republican Cybersecurity Task Force. 2011. "Recommendations of the House Republican Cybersecurity Task Force." Washington.

[27] Manfra, Jeanette. 2017. The White House Press Briefing. "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea" https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

Cybersecurity and Communications and Integration Center (NCCIC) and the Automated Indicator Sharing (AIS) program, which has been afforded legal liability protections under the Cybersecurity Act of 2015.

In addition, government can benefit from industry sharing more technical information on how private entities are structured and their exposure points so the Federal Government can obtain a better strategic view for *Collective Defense*. Industry can also identify effective risk analysis practices and share further knowledge with government. Improving upon information sharing and expanding the dissemination of indicators can help improve *Collective Defense* and drive up costs for attackers. Government also has information to share, including best practices and valuable information from its unique vantage point.

Still, industry can also expand its information sharing among private sector partners through engagement in ISACs, Information Sharing and Analysis Organizations (ISAOs), and other information-sharing forums. Government and industry can collaboratively promote participation in ISACs and ISAOs, which can anonymize and share information with the government that companies do not want to share directly themselves. Industry and government could both undertake greater efforts to bring underserved critical infrastructure sectors into the information sharing fold. Industry can also inform government as to the type of cyber threat information which is most helpful to them. It is imperative that industry and government build on the current public-private partnership model to continue to create analyst-to-analyst relationships so that all types of information as well as context can be shared in an environment of trust. One example of this type of exchange is DHS's Cyber Information Sharing and Collaboration Program (CISCP). Industry could also share information with the USG on its own efforts to secure cyberspace including efforts to address current priorities and issues such as botnets, supply chain issues, and cloud security. Taken together, these various information sharing initiatives can contribute to an enhanced situational awareness among industry and government.

2. Innovate Creative Cybersecurity Solutions

Industry should partner with government to create cybersecurity research and development (R&D) objectives[28] to promote innovation and deployment of cutting-edge cybersecurity solutions that can keep up with the fast-paced cybersecurity threat. The National Critical Infrastructure Security Resilience (CISR) Research and Development Plan recommended R&D roadmaps include an "understanding of infrastructure systems— technological, physical, and natural—to include interdependencies and cascading effects."

A cybersecurity R&D plan should be detailed, address industry and government's role in implementation of an R&D agenda, and be regularly reviewed by relevant stakeholders. Additionally, some of the most important innovations are organizational rather than technical. Companies, cities and states should be encouraged to experiment with different organizational approaches to cybersecurity challenges. For example, at the state level, it may be valuable to bring together chief information officers (CIOs) or chief

[28] Business Software Alliance, Center for Democracy and Technology, U.S. Chamber of Commerce, Internet Security Alliance, Tech America 2011.

information security officers (CISOs) and National Guard/adjutant general staff organizations in active collaboration against cybersecurity threats, especially with a focus on better support to SMBs in their state.

Innovations should expand beyond simple technological developments to include tools for training boards of directors, such as the "National Association of Corporate Director's Handbook on Cyber-Risk Oversight". Guidance documents can be adapted for training on cybersecurity for government agency leaders and general counsels, among others. A more collaborative partnership on technology development may foster implementation of more reliable resources for *Collective Defense* and attribution.

3. Develop the Cybersecurity Workforce

A cybersecurity skills and jobs shortage has been plaguing both government and industry alike for many years. According to a 2015 analysis of numbers from the Bureau of Labor Statistics, more than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74% over the past five years.[29] The House Republican Cybersecurity Task Force Report identifies workforce development as a key area for improving cybersecurity. The report states "We should continue to advance educational and awareness initiatives to help meet this demand for the federal workforce, which, in turn, will benefit the private sector as well." Advancing this goal is a good step toward increasing our national security.[30] Current estimates place a shortage of more than one million cybersecurity jobs globally that will go unfilled.[31]

Additionally, the *Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future* report by DHS and The U.S. Department of Commerce which responds to EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure states that the "United States needs immediate and sustained improvements in its cybersecurity workforce situation" and how it's important to expand the pool of cybersecurity candidates by retraining those employed in non-cybersecurity fields and increasing the participation of women, minorities, and veterans as well as students in primary through secondary school.[32]

DHS is currently improving the Nation's cybersecurity human capital and the Federal Government's cybersecurity workforce by assisting America's academic institutions to produce qualified entry-level employees and increasing awareness of cybersecurity professional opportunities. Initiatives like the National Centers of Academic Excellence (CAE) Program which is jointly sponsored by DHS and the National Security Agency (NSA), and the Scholarship for Service (SFS) Program, which allows students to

[29] Morgan, Steve. 2016. Forbes: "One Million Cybersecurity Job Openings in 2016"
[30] House Republican Cybersecurity Task Force. 2011. "Recommendations of the House Republican Cybersecurity Task Force." Washington.
[31]Zadelhoff, van Marc. 2017. Harvard Business Review: "Cybersecurity Has a Serious Talen Shortage. Here's How to Fix It"
[32] The Department of Commerce and Department of Homeland Security. 2018. "A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future."

attend colleges and universities through scholarships funded by the National Science Foundation (NSF), are some of DHS's efforts to increase the cybersecurity workforce. Industry can also continue to play an important role in these efforts to promote cyber curriculums in environments that incentivize students to pursue and support national interests. The Nation needs an integrated, multifaceted, and targeted program with research-based messaging to encourage students to join the cyber workforce. Efforts should be cognizant of the overall perception of the career field and undertake creative approaches to incentivize new members to join the workforce.[33]

What Industry and Government Can Do Together

1. Identify and Manage Systemic Risks

The interconnectedness of our society and our reliance on critical infrastructure to maintain our way of life has led to the formation of systemic risks within our country. We must be more aware of single points of failure, concentrated dependencies, and cross-cutting underlying functions.[34] While DHS recognizes catastrophic risk through its designation of "critical infrastructure," systemic risk is notoriously difficult to define and categorize. Systemic risk can emerge across interconnected systems, resulting in harmful effects that could cascade into national security, public safety, and public confidence. Systemic risk is shared among multiple stakeholder groups, requires collective action to resolve and worst of all, the impacts are hard to predict. DHS is working to better understand systemic risk at a national scale.

It is imperative that government and industry come together and take immediate steps to gain a better understanding of how to frame the problem of systemic risk, develop a more robust picture of collective vulnerabilities, and clearly define it. Often systemic risk is not isolated to a specific industry or sector, thus managing systemic risk across sectors is imperative. Government and industry also need to work together to identify National Critical Functions (NCFs). By identifying and analyzing NCFs, government and industry may be able to provide insight to prevent current and future cyber-attacks on these targets.[35]

The interplay between physical and digital threats and consequences should also be analyzed. Aviation cybersecurity, undersea cable, positioning, navigation and timing (PNT), and supply chain areas are particularly susceptible and in need of analysis. In order to get ahead of the problem, a joint effort involving participation from the private sector and international partners is needed.

---

[33] Additional information about cybersecurity workforce development, training, and education efforts can be found on the National Initiative for Cybersecurity Careers and Studies (NICCS) website at https://niccs.us-cert.org.

[34] Nielsen, Kirstjen M. 2018. DHS: "Remarks at the RSA Conference" https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference

[35] The IT Sector has long used the term "Critical Functions" and engages in risk assessment activities to improve the resiliency of the sector, DHS may leverage previously gathered information by the sector as appropriate in its efforts to identify systemic risk and NCFs.

Understanding the systemic vulnerabilities built into the fabric of our country, as well as better conceptualizing our NCFs are both critical steps to obtain a comprehensive picture of national risk, and will allow us to proactively and collectively manage these issues.

2. Enhance and Expand Public-Private Sector Partnerships

While multiple lines of effort to achieve *Collective Defense* are needed, leveraging public-private partnership across all of them is essential to success. The NIPP states that the value of this type of partnership originates from the "direct benefits associated with a clear and shared interest in ensuring the security and resilience of the Nation's critical infrastructure" and goes on to state this value is maintained "throughout a network of national, regional, state, and local partnerships between government and owners and operators."[36] Much of the work and progress made towards our long-term security goals have come from these partnership structures and frameworks, including the Sector Coordinating Councils (SCCs), ISACs, the Critical Infrastructure Partnership Advisory Council (CIPAC), and the State Local Tribal and Territorial Government Coordinating Council (SLTTGCC) who "provides an organizational structure to coordinate across jurisdictions on State and local government guidance, strategies, and programs."[37]

Fully utilizing these partnerships and identifying areas where more collaboration is needed to achieve the goals will be necessary to protect critical assets and to build creative new ideas. It is also imperative to enhance the existing frameworks and policies government and industry have established, by honing the most effective ways to work in partnership. All partnership entities should reference the best practices for public-private partnerships as agreed upon by the IT SCC, which were endorsed by PCIS.[38]

Government and industry also need to work to expand on existing regional, state, and local partnership structures. As regional entities continue to mature and expand, DHS will need to leverage its expertise in the field, through its Cyber Security Advisors (CSAs) and Protective Security Advisors (PSAs), to continue to effectively collaborate with partners outside the National Capital Region. Government should also leverage the DHS Office of Infrastructure Protection (IP) "regional delivery model" which seeks to improve the delivery of services to critical infrastructure owners and operators from IP headquarters to 10 regional offices.[39] Additionally, government and industry should review best practices and successes from state government leadership examples, such as New Jersey's Office of Homeland Security and Preparedness council structure.

---

[36] Department of Homeland Security. 2013. "National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience." 11.

[37] Department of Homeland Security. 2013. "National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience." 12.

[38] Clinton, Larry. 2015. Journal of Strategic Security: "Best Practices for Operating Government-Industry Partnerships in Cyber Security."

[39] Department of Homeland Security. 2017. NPPD: "Regional Service Delivery Model Fact Sheet."

Conclusion

Our adversaries are not distinguishing between public and private, so neither should we; therefore, government and industry must work collectively now more than ever. DHS pursues a model of 'collective defense' in cybersecurity, meaning government and industry take collaborative, tangible actions together to mitigate threats and reduce the most serious, enduring and collective strategic cyber risks to the United States and to our international partners. Cybersecurity is a shared responsibility and only through public-private sector partnerships and collaborative efforts will we achieve *Collective Defense* of our cyber ecosystem. While our public and private sector partnership is by definition collaborative, it is necessary to reiterate that these efforts and the recommendations throughout this paper need to be driven and accomplished mutually. As Secretary Nielsen pointed out at the 2018 RSA Conference, "If we prepare individually, we will fail collectively."

Works Cited

Better Business Bureau. 2017. "2017 State of Cybersecurity Among Small Businesses in North America."

Business Software Alliance, Center for Democracy and Technology, U.S. Chamber of Commerce, Internet Security Alliance, TechAmerica. 2011. "Improving Our Nation's Cybersecurity through the Public-Private Partnership."

Center for Cyber and Homeland Security Active Defense Task Force. 2016. *Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats.* Washington: Center for Cyber and Homeland Security.

Cisco Security. 2018. *Annual Cybersecurity Report.* San Jose, CA: Cisco.

Clinton, Larry. 2016. *The Cybersecurity Social Contract: Implementing a Market-Based Model for Cybersecurity.* Internet Security Alliance.

Clinton, Larry. 2015. Journal of Strategic Security: "Best Practices for Operating Government-Industry Partnerships in Cyber Security"

Daniel, Michael. 2015. The White House Blog: "Strengthening Cyber Risk Management" https://obamawhitehouse.archives.gov/blog/2015/02/02/strengthening-cyber-risk-management

Daniel, Michael. 2014. The White House Blog: "Assessing Cybersecurity Regulations" https://obamawhitehouse.archives.gov/blog/2014/05/22/assessing-cybersecurity-regulations

Department of Homeland Security. 2018. "Cybersecurity Strategy."

Department of Homeland Security. 2017. NPPD: "Regional Service Delivery Model Fact Sheet"

Department of Homeland Security. 2016. "National Cyber Incident Response Plan USCERT" https://www.us-cert.gov/ncirp

Department of Homeland Security. 2013. "National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience."

Department of Justice. 2015. “Best Practices for Victim Response and Reporting of Cyber Incidents”

Duke, Elaine C. 2017. "Binding Operational Directive BOD 18-01: Enhance Email and Web Security." Department of Homeland Security.

Federal Trade Commission, Department of Justice. 2014. “Antitrust Policy Statement on Sharing Cybersecurity Information” 1-9.

Feeney, Christopher. 2017. US Senate Committee on Homeland Security & Governmental Affairs: “Cybersecurity Regulation Harmonization”

George Washington University. 2016. “Center for Cyber and Homeland Security Active Defense Task Force”

House Republican Cybersecurity Task Force. 2011. "Recommendations of the House Republican Cybersecurity Task Force." Washington.

Johnson, Derek B. 2017. *FCW.* October 24. https://fcw.com/articles/2017/10/24/bossert-mccain-hearing-stunt.aspx.

Levy, Ian. 2018. *Active Cyber Defence - One Year On.* UK National Cyber Security Centre.

Manfra, Jeanette. 2017. The White House Press Briefing. “Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea” https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

Marks, Joseph. 2017. *Nextgov.* December 19. http://www.nextgov.com/cybersecurity/2017/12/heres-why-trump-administration-called-out-north-koreas-cyberattacks/144694/.

Morgan, Steve. 2016. Forbes: “One Million Cybersecurity Job Openings in 2016”

National Association of Corporate Directors. 2017. “Handbook on Cyber-Risk Oversight”

National Security Telecommunications Advisory Committee. 2014. “Report to the President on Information and Communications Technology Mobilization” https://www.dhs.gov/sites/default/files/publications/ICTM%20Final%20Draft%20Report%2011-2014%20%282%29.pdf

Neus, Elizabeth. 2018. *FedTech.* February. https://fedtechmagazine.com/article/2018/02/dhs-jeanette-manfra-turns-her-focus-ecosystem-government-networks.

Nielsen, Kirstjen M. 2018. DHS: “Remarks at the RSA Conference” https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conferenceObama,

President Barack. 2013. "Improving Critical Infrastructure Cybersecurity." Washington, DC: Federal Register, February 12.

Pan-Industry Association. 2011. “Improving Our Nation’s Cybersecurity through the Public-Private Partnership”

SBA Office of Advocacy. 2017. “United States Small Business Profile” 1-4. https://www.sba.gov/sites/default/files/advocacy/United_States_1.pdf

Symantec. 2017. “Internet Security Threat Report” 1-77.

The Department of Commerce and Department of Homeland Security. 2018. "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats."

The Department of Commerce and Department of Homeland Security. 2018. “A Report to the President on Supporting the Growth and Sustainment of the Nation’s Cybersecurity Workforce: Building the Foundation for a More Secure American Future.”

Trump, President Donald. 2017. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." The White House.

United States Government. 2016. “A Unified Message for Reporting to the Federal Government”

Zadelhoff, van Marc. 2017. Harvard Business Review: “Cybersecurity Has a Serious Talent Shortage. Here’s How to Fix It.”