Cybersecurity Priorities

Recommendations for Fiscal Year 2019
The House Appropriations Committee
Subcommittee on Homeland Security

Prepared by
Congressman C.A. Dutch Ruppersberger
Spring 2018

Executive Summary

Over the past year, I have met with more than 50 different government, retired government and industry stakeholders to learn more about the Department of Homeland Security's cybersecurity mission, including its efficiency and effectiveness. I have pursued this as part of my role as a Member of the House Appropriations Committee, Subcommittee on Homeland Security. I appreciate the expertise and insight I have received over the last year from all involved. I look forward to continuing my work with all parties to defend our country against the threats we face every day, including in cyberspace.

The takeaways from these briefings, meetings and roundtables are contained in this Executive Summary and outlined in greater detail in the subsequent pages. I hope that the Subcommittee will take them into consideration when conducting its oversight of tax dollars at work executing the Department's cybersecurity mission. There is no doubt that many important issues, such as the integrity and security of our election systems, will be brought before the Committee throughout the process of drafting the Fiscal Year 2019 appropriations package. I consider the recommendations outlined in this document areas of additional focus for the Subcommittee.

The Department has many responsibilities, most of which are essential to our national security and economic prosperity. The Department is tasked with both providing cybersecurity to the civilian agencies that serve the American public daily and empowering the private sector to defend itself. That fact alone — the broad and critical span of the Department's current cyber-

related responsibilities — requires us to begin providing detailed and precise guidance, where necessary, now.

In this document, I propose the following recommendations:

1. The Subcommittee should hold its first cybersecurity-specific budget hearing during FY2019.

2. The Subcommittee should focus on the Department's efforts to protect against the threats posed by the leak of cyber capabilities (tools), for example, vulnerabilities and exploits.

3. The Subcommittee should focus on the Department's efforts to protect against the threats targeting industrial control systems, for example, the energy grid.

4. The Subcommittee should evaluate the merits of shifting funding for cyber research and development (R&D) from the Science & Technology Directorate (S&T) to the National Protection and Programs Directorate (NPPD), as proposed in the President's Budget for FY2019.

5. The Subcommittee should focus on the Department's efforts to improve all aspects of information-sharing to address systemic risk, supply-side risk and acquisition reform.

6. The Subcommittee should explore alternative organizational structures within the government to better execute the cyber mission.

7. The Subcommittee should evaluate the Department's implementation of President Trump's National Infrastructure Advisory Council (NIAC) recommendations.

First, because we are the Committee (Appropriations) that oversees and funds the Executive Branch, I believe it is imperative that the Subcommittee hold a cybersecurity-specific budget hearing during FY2019. The Department must provide witnesses at

the appropriate level of responsibility and seniority who can speak to the cybersecurity mission programs specifically and take course-correcting actions identified by the Subcommittee. Receiving a proper budget hearing from the Department would be a good first step for the Subcommittee in solidifying our interest in, and ability to, ensure the success of this mission.

Second, I recommend the Department focus its efforts on protecting the .gov domain and the private sector from threats posed by the leak of cyber capabilities reportedly developed by major nation-state actors. Over the past few years, many advanced tools have become public and are currently being repurposed by both nation-state and non-nation state players. Protecting the public and private sectors against the capabilities they enable is imperative. The Administration undertook a review of the Vulnerabilities Equities Process (the process it uses to determine when to disclose a vulnerability to the private sector) in 2017. The Subcommittee should ensure that the Department is properly postured and funded to quickly and effectively mitigate any threat to the .gov domain and to work with the private sector to respond to the threat posed by these vulnerabilities and subsequent exploits.

Third, I recommend the Subcommittee review and ensure the Department is equipped to assist the private sector as it looks to address threats targeting the country's industrial control systems, including energy, water, and manufacturing entities in a range of categories. We've seen the emergence of concerted efforts targeting industrial control systems worldwide in recent years. This has been for both access and potential exploitation. A cybersecurity firm recently reported the presence of malware targeting industrial safety systems (designed to protect human life), raising serious concerns about the advancing capabilities of nation-state actors and their willingness to use them.

Fourth, in the President's Budget (PB) for Fiscal Year 2019, there has been a shift in the mechanism for funding cybersecurity R&D from S&T to NPPD - which is the operational side of the

Department's cybersecurity business. While there may be advantages to such a shift, the Subcommittee should carefully evaluate this change and ensure it will still allow the R&D team to produce the same high-yield products it has in the past and improve the Department's overall functioning in this critical area. There are obvious questions about whether a research agency housed in an operations-driven unit will be able to maintain the necessary flexibility to tackle complex, long-term problems – it is critically important to assure we stay ahead of adversarial nation-state actors in this domain, such as Russia, China, Iran, and North Korea.

Fifth, as the Department's Assistant Secretary for Cybersecurity and Communications recently indicated, there must be a serious evaluation of the effectiveness of the current automated cyber threat sharing initiatives available to the private sector, which owns and operates over 80 percent of U.S. networks. We can no longer rely solely on reactive indicator-based sharing programs to protect against and deter increasingly sophisticated threat-actors that are rapidly adapting and changing their tactics, techniques and procedures. Government agencies and industry need to develop and deploy better, more meaningful threat intelligence that communicates context of impact and furthers prioritization efforts to ensure greater resilience for their information and networks.

Similarly, the Department needs to better leverage relationships with the private sector to take advantage of the leading-edge platforms and resources it is developing and deploying. It is also critical that the government finally make good on its promise to demonstrate a value to the private sector in sharing threat intelligence. Discussions on moving information sharing to a robust, real-time environment in which the government and industry can develop a common operating picture of the threat landscape have gone on far too long.

Sixth, the Subcommittee should focus its oversight in the near-term on ensuring that the Department is properly set up to help

execute this mission and evaluate whether alternative structures may more effectively achieve our long-standing goals. Close attention should be paid to the ongoing recommendations within the Department with respect to the restructuring and increased operationalization of the National Protection and Programs Directorate. These may include some important benefits, which must be weighed against the very real challenges the Department faces in this area. The Subcommittee should also assist the House Committee on Homeland Security in its efforts to reorganize the Department.

While the Department's leadership has important cyber experience, longer-term issues about the Department's capacity to execute this critical mission for the nation continue to be of concern. We should continue to ensure that the government is making the best, most effective use of its capabilities and assets to help defend both the .gov domain as well as, perhaps even more importantly, the American private sector. In the long-run, this may require a fundamental restructuring of how the government addresses these issues, both functionally and structurally.

Finally, the Subcommittee should evaluate the extent to which the Department is working to implement key recommendations made by the President's NIAC report, released in August 2017. Many of the NIAC report's recommendations would help address the issues identified in this report and the Subcommittee should evaluate whether appropriate resources are currently being allocated to support such efforts.

It is my hope that the Subcommittee seriously consider all the recommendations outlined in this document.

Think Big

As the former Ranking Member of the House Permanent Select Committee on Intelligence and the Representative of the Congressional District that is home to the National Security Agency (NSA), I have been intimately involved with the progression and growth of our nation's classified cybersecurity programs over the last decade.

There must be better collaboration between the Intelligence Community (IC) and the Department of Homeland Security to protect the private sector from the advanced and persistent cyber threats of today and tomorrow. Former Deputy Director of the NSA, Chris Inglis, effectively outlines the current issue when comparing the U.S. to the United Kingdom's new National Cyber Security Centre (NCSC), which was created to enhance the IC's partnership with the private sector:

> "Today, in the United States, it works the opposite [of the NCSC]. Most of our government's national security cyber sleuths live in a classified world where people at the NSA, CIA, and FBI have to make a determination of what will be released from the classified domain. That creates a much harder and steeper slope for someone to chime in, justifying the merits of sharing something from a smaller to a larger audience."[1]

I believe this Subcommittee should evaluate the Department's ability to effectively leverage IC capabilities to deliver real-time benefits to the private sector. The Department should also seek more actionable information from the IC to more fully and effectively utilize the Department's existing intelligence-related office and resources. Or, perhaps the Department would be best postured as a middle man: providing links to IC resources and facilitating direct interaction between the private sector and the IC. This could potentially improve the timeliness, effectiveness and

[1] *U.S. Cyber Survival Depends on Greater Collaboration*, Chris Inglis. The Cipher Brief, June 21, 2017. https://www.thecipherbrief.com/column_article/u-s-cyber-survival-depends-on-greater-collaboration

speed of the government's response to attacks targeting the private sector in planning or in progress.

The Subcommittee should also work with the full Committee on Appropriations, and the Committee on Homeland Security, to assess whether our current functional and structural model in the Executive Branch is effective in carrying out the national-level domestic cybersecurity mission. Today, the Department has a very broad and diverse mission on its plate and it has become clear that it continues to face significant and daunting challenges when it comes to effectively fulfilling its cybersecurity mandate. The capable cybersecurity professionals at the Department may need to be elevated significantly — more so than under the current NPPD reorganization proposal. The Subcommittee, working with the full Committee, should also consider how the government as a whole should structure itself to best address these issues. We should remain open to the idea of removing the mission from the Department and creating a new, Executive-level agency with the exclusive purpose of carrying out our nation's domestic cyber defense goals.

As General Keith Alexander, the former Director of the National Security Agency, Founding Commander of U.S. Cyber Command, and current CEO of IronNet Cybersecurity, co-wrote last year for the Federal Times' Fifth Domain:

> "While nation-states have long sought access to the critical systems of other nations for espionage and similar purposes, we've now seen an expansion to more aggressive actions, ranging from large-scale theft of private sector information for economic advantage, to the use of actual destructive attacks that have effects in both cyber and physical space. And while this activity is taking place at a relatively low rate at this time … the potential impact of these threats on our industry and government highlight the need to focus on our joint cyber defense. Specifically, we must fundamentally rethink how the private and public sectors interact in cyberspace and recast the way in which we think of the respective roles of departments and agencies

within the government and how they interact with private entities.[2]

The cybersecurity threat in 2018 knows no bounds and spans across almost every sector of industry in our country and those of our allies. If we do not seek ways to strengthen and improve upon current authorities across the IC and the Department, in tandem with directly empowering the private sector, we may not be able to prevent and possibly respond to a large-scale systemic or catastrophic cyber-attack.

Recommendations

Cybersecurity Budget Hearing

The President's Budget for FY2019 says that, "DHS cybersecurity programs are more important than ever."[3] The Department receives more than $3 billion for its cybersecurity mission.[4] In order to ensure the use of these tax dollars is consistent with the priorities set by this Subcommittee and to better understand the effectiveness of the Department's major programs, we must be briefed in a substantive manner.

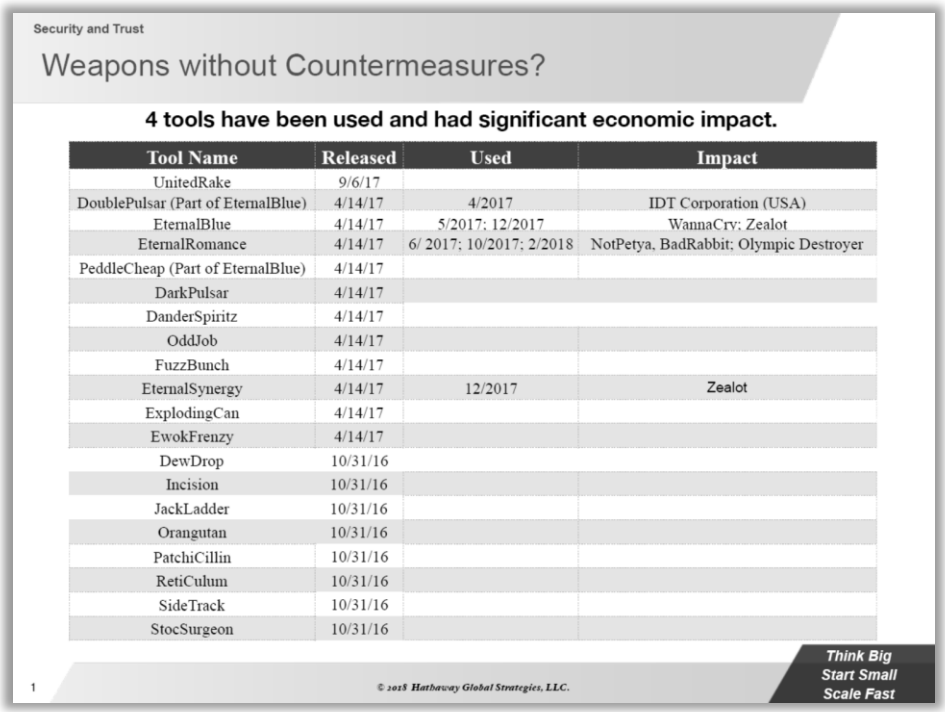
Therefore, the Subcommittee should request a cybersecurity-specific budget hearing from the Department. This budget hearing should include relevant officials at the appropriate level of responsibility and seniority who can speak to the allocation of cybersecurity resources within the Department at-large and the National Protection and Programs Directorate, specifically.

[2] *See* Keith B. Alexander & Jamil N. Jaffer, *Architecting the Nation for Cyber Defense*, Federal Times Fifth Domain (Jan. 10, 2017), available online at <https://www.fifthdomain.com/home/2017/01/10/architecting-the-nation-for-cyber-defense-commentary/>.
[3] *An American Budget*, Office of Management and Budget. PG 59. https://www.whitehouse.gov/wp-content/uploads/2018/02/budget-fy2019.pdf
[4] The President's request for the National Protection and Programs Directorate for FY '19 is $3.348 B

Concentrate focus on countermeasures against leaked cyber tools

In recent years, highly advanced cyber capabilities have been appearing in the wild, purportedly stolen from nation-states. Since, other nation-states and their proxies, as well as criminal actors, have sought to repurpose these tools to their nefarious ends. The weaponization of these tools by malicious actors poses a significant risk to the U.S., our allies and the American private sector.

As shown in the following chart, four cyber tools stolen in a single theft have had significant economic impact. Many other tools stolen in the attack remain unused – the threat still looms. The Subcommittee must ensure that the agencies in charge of coordinating defense against these capabilities, including the Department, are properly tasked and resourced so that they can quickly and effectively mitigate threats to the .gov domain and private sector networks.



[5]Graphic provided by Hathaway Global Strategies, LLC.

The Subcommittee might also consider whether direction is appropriate to guide the government's effective use of the Vulnerabilities Equities Process (VEP). This process seeks to:

> "balance whether to disseminate vulnerability information to the vendor/supplier in the expectation that it will be patched, or to temporarily restrict the knowledge of the vulnerability to the USG, and potentially other partners, so that it can be used for national security and law enforcement purposes, such as intelligence collection, military operations, and/or counterintelligence."[6]

In 2017, the National Security Council released a report to the public to both promote transparency and respond to concerns from the private sector that the government could decline to disclose vulnerabilities it discovers in their products.

The government can better effectuate ongoing intelligence operations, in many cases, by withholding vulnerabilities from the private sector. However, government workers and policy makers need better guidance when it comes to finding the balance sought by the VEP. The Subcommittee should recognize the Department's long-standing expertise and role assessing and coordinating vulnerability disclosure and ensure the Department is prioritizing its VEP funds to evaluate threats that are already publicly disclosed or likely to become public in the near future.

Industrial Control Systems (ICS) Security

Public reports have made clear that the threats to our nation's most critical infrastructure, as well as those of our allies, are not only increasing in volume and frequency, but in sophistication.

In fact, public reports indicate there were more than 6,000 cybersecurity incidents and five nation-state teams targeting industrial systems specifically in 2017 alone.[7] Last year, we learned about the first scalable malware that can ostensibly disrupt

[6] *Vulnerabilities Equities Policy and Process for the United States Government*, The White House. PG 1. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

[7] Figures provided by Dragos, Inc. and will later be published in a 2017 ICS threat landscape document.

electric grids as well as the first malware specifically designed to attack industrial safety systems, which are purposefully designed to protect human life.

Our adversaries understand this is an area primarily owned and operated by the private sector. The diversity of ownership, and varying levels of security capability at each entity, make it hard for the Department to predict future attacks and help respond effectively, especially within the operational technology – such as the physical switches and breakers that make up the electric grid.

Just as troubling, public reporting suggests that our adversaries are using smaller energy, water, and other key infrastructure targets as their "training" grounds. That's because these smaller entities have less resources for cyber defense compared to their larger, corporate counterparts.

The Committee should ensure that relevant teams within the Department are properly equipped to tackle the increasing threats to the 16 critical infrastructure sectors, including those on the Section 9 list (entities of critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security).[8] The Subcommittee should consider funding additional Department work on protecting industrial control systems (ICS) and other operational technology (OT), particularly given the extensive use of such systems in critical infrastructure facilities.

The Subcommittee should consider development of a system that will provide cross-sector visibility, in real time, into cybersecurity incidents that occur in U.S. critical infrastructure. This capability would have the ability to assess potential impacts to critical infrastructure ICS from detected intrusions.

[8] As defined in President Obama's February 2013 Executive Order. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Dragos Inc., a Maryland-based ICS/OT specific cybersecurity firm in my Congressional District, points out the problem well:

> "The most frequently reported attack vector used against industrial infrastructure environments is actually 'unknown' because both asset-owner and governmental security teams have generally lacked adequate staff and ICS-focused technology to identify them."[9]

The Subcommittee should, therefore, evaluate whether the Department needs more resources for the express purpose of better understanding the threats posed to critical infrastructure systems, especially at smaller energy, water and other infrastructure companies. The Subcommittee should also consider whether these funds should be funneled directly to states and localities, who can better determine how to allocate them. To that end, the Subcommittee may wish to establish a grant program for any new funds in this area.

Research & Development (R&D)

The President's Budget for FY2019 creates a new protocol for the funding of the Department's Cybersecurity Research and Development (CSD) mission.

This mission has traditionally fallen under the Science and Technology Directorate, however, in FY2019 and moving forward, this mission will be moved to the National Protection and Programs Directorate, where the operational cyber mission is housed. In addition to maintaining proper allocation of resources, the Subcommittee should evaluate how this shift will affect the research and development goals of the Department and work to ensure that CSD can continue to help the private sector commercialize innovations.

The CSD mission is currently tasked with solving a range of big and complicated problems (for example, aviation cybersecurity) and the Subcommittee should examine whether large-scale, long-

[9] *The Dragos ICS Cybersecurity Ecosystem: Safeguarding Civilization*, Dragos, Inc. PG 2. https://dragos.com/media/Corporate_Brochure.pdf

term projects like these – which are critically important to our national security – will continue to thrive in an operationally-driven research and development environment. The Subcommittee should hear from various stakeholders to evaluate the best path forward.

The Subcommittee should also consider enhancing resources for CSD to focus on additional forward-leaning projects, such as improving the security of computer code. A recent roundtable held by the Cyber, Space, and Intelligence Association and the Cyber Threat Alliance, which I participated in, produced some potential areas of focus for future R&D projects including:[10]

- Better code creation (for example, security, quality) – including reducing the number of exploitable vulnerabilities per line of code.

- Supply chain – enabling vendors or third-party reviewers to verify hardware and software security throughout the acquisition and systems engineering life cycle.

- Secure communications – reducing the weaknesses inherent in the software protocols that make the Internet function.

- Artificial Intelligence and Machine Learning – understanding how AI/ML could be used to enhance both offensive and defensive cybersecurity capabilities.

- Data manipulation, and data corruption defenses – developing the capability to defend against "spoofing", data manipulation, and data corruption in multiple types of IT systems.

- Cybersecurity workforce – improving cybersecurity training for the workforce as well as methods for identifying, reporting, and tracking suspicious behavior.

[10] These recommendations include information and recommendations in an internal document provided by the Cyber, Space and Intelligence Association and the Cyber Threat Alliance to Congressman Ruppersberger.

The Subcommittee should ensure that these changes to CSD are not to the detriment of our ability to stay ahead of our adversaries in this space.

Information Sharing

The Department currently has an information sharing portal, known as Automated Indicator Sharing (AIS), which was developed under the authority of the *Cybersecurity and Information Sharing Act of 2015*. Many private sector groups have raised concerns about this program and the benefits it is supposed to provide to subscribers of its threat indicator stream.

Although it controls 80 percent of our country's networks, the private sector continues to share only limited threat data with the government because it sees little value in the information it receives from the government. A roundtable discussion with several organizations identified the following deficiencies with regards to the AIS program:[11]

- The current indicators shared through the AIS program often lack the contextual information needed to tell which items are relevant.

- The AIS program lacks a mechanism to enhance data already shared. If a company discovers more cyber threat intelligence related to a previously shared indicator and wants to update the shared information, they are unable to do so.

- The AIS program does not vet its published indicators, which can result in a great deal of "noise" its subscribers must sort through. This raises the cost of the program for all participating organizations.

[11] These recommendations include information and recommendations in an internal document provided by McAfee to Congressman Ruppersberger.

- Becoming an AIS participant is extremely burdensome. The need to have corporate lawyers involved at multiple points in the application and onboarding process makes it challenging and costly for corporations.

- The private sector would see more value in participating if it knew the U.S. government was also actively sharing information. Currently, it is not possible for the private sector to determine which information has been provided by the U.S. government.

In order for the AIS program to be successful, it must be mutually beneficial. The Department needs to find ways to make this happen to improve the cycle of defense across the American cyber ecosystem.

According to Jeanette Manfra, the Assistant Secretary for Cybersecurity and Communications, the Department is planning to update the program later this year in an effort to address some of the problems described above, especially threat context. The Subcommittee should evaluate any proposed changes and, as appropriate, provide resources and guidance on these efforts. Once such efforts are underway, the Department should brief the Subcommittee on its implementation plan.

The Subcommittee could also work with the full Committee and relevant authorizing Committees to consider legislation improving upon CISA as passed in 2015. Considerations should include offering the private sector proper liability protection and incentives for sharing threat data with the government. This includes stronger regulatory protections and lessening the minimization burden, while ensuring adequate privacy protections, on the private sector.[12]

Furthermore, the Subcommittee should consider how it can help the Department create a standardized format used to share

[12] *See, e.g.*, Jamil N. Jaffer, *Carrots and Sticks in Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015*, 67 S. Car. L. Rev. 585, 589-97 (Spring 2016).

information between government agencies and the private sector. An interoperable communication "template" will help all parties adapt and respond more effectively.

Cyber Roles & Responsibilities

Evaluating the proper role and allocation of cyber responsibilities across the federal government is a critical, long-term need of our nation. The Subcommittee can begin by undertaking a detailed review of the Department's proposed restructure under the NPPD, which, hopefully, will enable the Department to rapidly scale and improve its capabilities. Achieving this goal may require a new set of authorities and responsibilities, including potential new government structures.

Implementation of NIAC Report

In August 2017, the President's National Infrastructure Advisory Council (NIAC) issued a report with recommendations for improving our national cyber defenses, including some that would address the issues identified in this document. As such, the Subcommittee should closely examine the NIAC recommendations, evaluate whether the Department has begun implementation of any and the extent to which that implementation has been effective. There are three recommendations specifically directed at the Department that could merit Subcommittee resources and guidance:

1. Facilitating a private-sector-led pilot of machine-to-machine information sharing technologies;

2. Using ongoing national-level exercises to test the execution of federal authorities and capabilities during cyber incidents and to clarify the federal government's response and authorities; and

3. Establishing clear protocols to more effectively and rapidly declassify cyber threat information and proactively share it with owners and operators of critical infrastructure.

In addition, the NIAC made three key broader recommendations that the Subcommittee should work with the full Committee and Department to assess and, as appropriate, fund:

1. Establishing limited-time, outcome-based market incentives that encourage owners and operators to upgrade cyber infrastructure, invest in state-of-the-art technologies, and meet industry standards or best practices;

2. Streamlining and significantly expediting the security clearance process for owners of the nation's most critical cyber assets, and expediting access to SCIFs; and

3. Piloting a taskforce of experts in the government and key industries to take decisive action on the nation's top cyber needs.

Conclusion

Every mission assigned to the Department – from securing our borders both physical and digital, to defending our critical infrastructure – is immeasurably important. The Subcommittee should exercise its oversight authority to ensure that the Department's missions are properly funded and executed. We need to send a clear message to the Department and its leaders that this Committee is interested in all of its many missions to protect our nation.

Staff Contact

Elliott R. Phaup, Policy Advisor
Elliott.Phaup@mail.house.gov
202-225-3061

Media Contact

Jaime Lennon, Director of Communications
Jaime.Lennon@mail.house.gov
410-628-2701