Input to the Commission on Enhancing National Cybersecurity

RFI Response: Information on Current and Future States of Cybersecurity in the Digital Economy

Author: J. E. Shaffer

Summary Recommendations:
1. Continue to champion a risk-based approach to cybersecurity.
2. Develop and operationalize cybersecurity red teams.
3. Anticipate effects-based cybercrime and cyberwarfare.
4. Continue to mature the concept of cybersecurity as a public good.
5. Build an insurance model based on threat profile and cybersecurity capability maturity.
6. Consider crowdsourcing cyber surety testing.
7. Facilitate the transition of personnel between government, the private sector and academia.
8. Adopt the healthcare model for cybersecurity practitioners.
9. Embrace the modern work culture for hackers and technology professionals.

1. Continue to Champion a Risk-Based Approach to Cybersecurity
Related Topics: *Critical Infrastructure Cybersecurity, Federal Governance, Internet of Things, State and Local Government Cybersecurity*
Focus Areas: *Government, Private Sector*
Discussion: In recent years, the Federal Government and much of the private sector have transitioned from a control-centric to a risk-based approach to cybersecurity. For example, in 2014 the DoD began the transition from the DIACAP process to the Risk Management Framework for security assessments for technology acquisition and development. This trend should continue in a manner that is not designed to completely supplant a controls-based approach, but rather to work harmoniously and in concert with the ontology of existing controls identified in NIST, CSC, ISO, and other standards organizations. A risk-based approach provides the best means to strike a balance between business needs and protecting critical assets and infrastructure. A continuous risk assessment process requires an organization to identify the critical assets (including information, system, facility, personnel, and financial) required to accomplish its mission essential tasks, identify the vulnerabilities and weaknesses that may be exploited to harm those assets, and monitor the threats that may target those assets for exploitation, theft, or damage. The end result is an asset-focused security posture that is optimized across the full spectrum of security controls (i.e. Identify, Protect, Detect, Respond, and Recover), tailored to the threats faced by the organization, and constantly reassessed as both the threat and organization evolve.
Recommendations:
1. *(Government)* Build a cadre of security professionals trained and experienced in information security risk management who are responsible for the continuous assessment of the information security risk for federal organizations.
2. *(Government)* Reinforce the risk-based approach in standards and governance, and help understand how organizations can harmonize the risk-based approach with existing controls.
3. (*Government)* Continue to transition the cybersecurity and information assurance assessment process away from traditional “controls checklist” approaches and towards an approach that is tailored to an organization's specific risk posture.
4. (*Private Sector)* Leverage the expertise of traditional risk management functions within financial, insurance, and other organizations to assist the government in maturing a risk-based approach to cybersecurity.

2. Develop and Operationalize Cybersecurity Red Teams

Related Topics: *Cybersecurity Workforce, Critical Infrastructure Cybersecurity, Federal Governance, Internet of Things, State and Local Government Cybersecurity*

Focus Areas: *Government, Private Sector*

Discussion: While much emphasis has been placed on shifting to a more proactive cybersecurity model, many organizations within the government and private sector remain in a constant reactive "firefighting" mode. Employing full-spectrum cybersecurity red teams can help shift the balance to a more proactive approach by emulating threats, probing existing security controls, and challenging organizational assumptions regarding cybersecurity (notionally and practically). A full-spectrum red team should be able to simulate everything from Chaos Monkey-type scenarios to current APT tactics, and (as the mission dictates) execute operations that span the physical, human/social, and network/system aspects of cybersecurity. Ideally, the red team should consist of a mix of offensive and defensive cybersecurity professionals, creative "out of the box" thinkers, and personnel with knowledge and experience in the target industry or sector. Selection of red team members should also consider maturity, as it is vital that the red team assessment is treated as an exercise in organizational growth and development rather than simply to highlight the weaknesses of an organization's security program. The red team approach can help organizations think outside of the box when it comes to implementing and prioritizing cybersecurity controls, and aids cybersecurity practitioners in tailoring cybersecurity requirements to the organization's mission and core functions. Moreover, the red team model is synergistic with the risk-based approach; red teams can both test controls surrounding known and existing risks as well as aiding the risk management process by identifying previous unexplored areas of risk.

Recommendations:

1. *(Government/Private Sector)* Develop shared guidelines and recommendations for the organizational structure, skills, and responsibilities for a full-spectrum cybersecurity red team.
2. *(Government/Private Sector)* Develop specific recommendations and guidelines for how to employ cybersecurity red teams within an organization while minimizing the impact to operations and collateral damage.
3. *(Government)* Leverage talent from existing Federal red teams to establish a red team training capability for both government and private sector organizations.
4. *(Academia)* Develop and deliver red team-focused courses as part of existing cybersecurity curricula.

3. Anticipate Effects-Based Cybercrime and Cyberwarfare

Related Topics: *International Markets, Cybersecurity Research and Development*

Focus Areas: *Government, Private Sector*

Discussion: In discussing the implications of the DNC hack with NPR's David Greene, Admiral Mike Rogers cautioned "you're now seeing people attempting to use information as a way to influence, strategically, specific events and directions" [Mor2016]. Inherently, as global interdependence on information and information systems continues to rapidly expand, so will the potential for exploitation by malicious actors. What Admiral Rogers alludes to is that such malicious action will go beyond the transactional cybercrime we see today and incorporate strategic decision-making with goals surpassing the tactical malicious actions that are executed. In anticipating this paradigm shift, we must learn how to better understand the second and third order effects of a particular malicious act. As cybercriminals continue to evolve into sophisticated organizations that mimic corporate operations, actions like hacking into a bank, executing a denial of service attack, stealing data, or defacing a website may become simply a means to an end. For example, a criminal organization may use analysis of previous attacks to predict how the stock price of a publicly traded company might be impacted by the defacement of that company's website. While this relatively low risk, low cost act will likely not be

extensively investigated or prosecuted, the perpetrators may benefit substantially based on accurately calculating how the market will respond. Especially challenging may be this type of strategic gambit that hinges upon virtually undetectable tactical actions. For example, imagine the impact of a small modification to the source code of a product that results in kinetic malfunctions and a corresponding safety recall for that product. The root cause of the malfunctions may be discovered only after extensive investigation (if at all), and there may be little impetus to connect the dots to identify the strategic beneficiaries of this action.

Recommendations:

1. *(Government/Private Sector)* In building organizational red team capabilities, ensure that adversary emulation and threat modeling practices incorporate both tactical and strategic operations.
2. *(Government/Private Sector)* In conducting investigations of cybersecurity incidents (or kinetic malfunctions/safety violations with cyber components), consider both the immediate and ultimate beneficiaries of the action.
3. *(Government)* Continue to develop methods for the accurate attribution of cyber criminals, even if prosecution is difficult or impossible.
4. *(Government)* Continue to build international law enforcement and prosecution capabilities such as to limit cyber criminals' freedom of maneuver.

4. Continue to Mature the Concept of Cybersecurity as a Public Good

Related Topics: *State and Local Government Cybersecurity, Public Awareness and Education*

Focus Area: *Government*

Discussion: While the cybersecurity industry continues to provide a significant boost to the US economy, there will always be some aspects of cybersecurity that are best handled by government entities. First, relying on the free market to drive businesses to prioritize security requirements is untenable; businesses are often willing to take risks in this area especially if the costs of a hack or data breach can be passed on to other entities (such as partners or customers). Second, cyberwarfare and cybercrime are inherently asymmetric. At a technical level, adversaries attempt to find the weaknesses in an organization's networks and infrastructure and aggressively exploit them. From a broader perspective, adversaries seek to find the “low hanging fruit” that allows them to accomplish their objectives; i.e., the organization with the weakest security posture. As the federal government and large businesses mature their cybersecurity capabilities, adversaries will increasingly target smaller organizations in order to achieve their objectives or leverage them as a springboard to exploit trust relationships with larger organizations. In the face of well-resourced cyber threats, the array of options available to small and medium businesses (SMB), educational institutions, and nonprofits is somewhat limited. This construct is shifting to a degree as security companies are catering more advanced capabilities and “security-as-a-service” models to the SMB, educational institutions, and nonprofits. However, there will likely always be capability gaps given the limited resources that SMB and smaller organizations have available to allocate to cybersecurity. To a degree, government-driven or government-supported compliance programs (such as HIPAA and PCI) help to prioritize security requirements in some industries; however, too often these simply become “check the block” exercises that deviate from their intended purpose. Thus, a re-examination of some of the “public good” aspects of cybersecurity is likely warranted.

Recommendations:

1. *(Government)* Evaluate the degree to which existing capabilities can be leveraged to support private sector cybersecurity needs. For example, consider the possibility of deploying a National Guard CND team to provide incident response to a cyber attack in a similar manner to providing humanitarian/disaster relief in the event of a natural disaster.
2. *(Government)* Create incentives for the expansion of cybersecurity products and services

catering to individuals, nonprofits, educational institutions and SMBs.

3. *(Government/Private Sector)* Build and encourage the growth of nonprofits chartered to assist individuals, nonprofits, educational institutions and SMBs with creating effective cybersecurity programs.

5. Build an Insurance Model Based on Threat Profile and Cybersecurity Capability Maturity.

Related Topic: *Cybersecurity Insurance*

Focus Area: *Private Sector*

Discussion: The idea of a cybersecurity insurance offering was introduced well over a decade ago, but for a variety of reasons its establishment has been slow. Developing an insurance model based on a consistent assessment of information security risk and cybersecurity maturity may assist in overcoming the current inertia and confusion hampering the widespread adoption of cybersecurity insurance. Creating a standardized assessment process that accurately gauges both the internal and external factors influencing an organization's security risk level will help to establish cybersecurity insurance as a viable option. From an internal perspective, insurers should evaluate the maturity of an organization's security program using a standard set of factors. The Cybersecurity Capability Maturity Model (C2M2), developed by the Department of Energy, provides an example of such an assessment. Maturity is a better gauge of an organization's security posture than traditional compliance checklists; maturity provides a more accurate measurement of an organization's security "health" in that it factors in concepts like organizational resiliency, risk management, metrics collection, and process improvement. From an external perspective, insurers should build threat profiles that consider factors like company size, industry segment, asset value, and geographical footprint to arrive at a relative threat score. To some degree, while the maturity score will incorporate factors that are within the locus of control for the organization, the threat profile score will account for the remaining factors that influence an organization's overall risk level. In considering the mechanisms to measure both internal and external factors, insurers should seek to leverage technology solutions to generate or enhance the validity of the assessed organization's maturity and threat profile scores. A simple example might be to deploy an email security gateway to evaluate the relative prevalence of targeted phishing attempts against an organization.

Recommendations:

1. *(Private Sector)* The insurance industry (specifically cybersecurity insurance providers) should identify, test, and deploy a standardized model for assessing the security maturity and threat profile for an organization.
2. *(Private Sector)* Identify and validate technology solutions suitable for assisting in the process of assessing the maturity of an organization's cybersecurity program or gauging the organization's threat profile.

6. Consider Crowdsourcing Cyber Surety Testing

Related Topics: *Internet of Things (IoT)*, *Cybersecurity Workforce*

Focus Area: *Private Sector*

Discussion: The Underwriter's Laboratory (UL) recently launched its Cybersecurity Assurance Program (CAP), which offers "testable cybersecurity criteria for network-connectable products and systems to assess software vulnerabilities and weaknesses, minimize exploitation, address known malware, review security controls and increase security awareness" [UL2016]. This is a promising and needed approach to addressing the safety and security concerns surrounding the IoT. However, the traditional model for product safety evaluation may be untenable given the existing backlog of technology requiring evaluation and the explosion of IoT devices and technologies. A crowdsourced approach might aid in bringing the numbers and mix of talent professionals to the table. The approach may need to be refined to transition from a "best effort" bug bounty approach to a more rigorous

process for cyber surety evaluation; for example, the broad community of security researchers may complete the majority of the technical work for a particular product and pass it along to UL for final evaluation and certification.

Recommendations:

1. *(Private Sector)* The UL should consider augmenting the CAP via crowdsourcing some components of its evaluation process. In doing so, it could adopt a model similar to BugCrowd or some corporate bug bounty programs such that the technology being assessed/tested is linked to a group of skilled vulnerability researchers who have experience with that technology.
2. *(Government)* Evaluate crowdsourced vulnerability research organizations to determine existing capabilities and suitability for OSHA-type safety and surety testing for IoT.
3. *(Government/Private Sector)* Work with UL and other organizations to develop a standardized methodology for testing the safety and security of IoT devices. Additionally, develop a set of qualifications for the personnel participating in the testing of these devices.

7. Facilitate the Transition of Personnel between Government, the Private Sector and Academia

Related Topic: *Cybersecurity Workforce*

Focus Areas: *Government, Private Sector, Academia*

Discussion: Other industries have experienced the exchange of knowledge, technology sharing, and innovative benefits derived from the synergistic flow personnel among the government, private sector, and academia. A typical model might offer professionals exposure to basic and applied research in academia, experience in technological innovation and application within the private sector, and overseeing the widespread adoption and scale of a technology or innovation within the government. To some degree, the cybersecurity industry benefits from this approach in leveraging existing programs designed to encourage this type of movement of skilled professionals. However, it may be worth re-examining the effectiveness of this process in the cybersecurity realm as the existing model may lack the requisite agility to keep pace with the current operational environment and technological innovation. Currently, the model seems to be a bit unbalanced, whereby government cybersecurity expertise (especially among servicemembers) readily flows into corporate roles and academia, but seems to be only a trickle in the other direction. Establishing or expanding programs designed to improve the movement of skilled personnel in all directions should help to even this out.

Recommendations:

1. *(Government)* Create or refresh existing programs to allow civilian and military professionals to pursue academic and/or private sector enrichment experiences in the cybersecurity realm. For example, a civilian cybersecurity analyst might be given the opportunity to leave the government, work in an equivalent role in the commercial sector for a set period of time, and return to his/her job (or equivalent) following that time period.
2. *(Private Sector)* Partner with government entities to best determine how to streamline the process of hiring and integrating skilled military and government civilian cybersecurity professionals into the workforce. Determine the roles and skill sets that are best suited for a fixed time period and reasonable transition from an equivalent government position.
3. *(Government/Private Sector/Academia)* Partner to develop a more standardized set of criteria for defining the knowledge, skills, and abilities required for various cybersecurity workforce roles.
4. *(Government)* Consider expanding the number of nonstandard and excepted service positions for qualified cybersecurity professionals.

8. Adopt the Healthcare Model for Cybersecurity Practitioners

Related Topic: *Cybersecurity Workforce*

Focus Area: *Government (Military-Centric)*

Discussion: In order to attract and retain a skilled cadre of healthcare professionals, the Services adopted a number of personnel management approaches that differ from that of standard members of the workforce. For example, physicians are often eligible for direct accession as an officer, offered time- and skill-based financial bonuses, evaluated under a different system for promotion and retention, and allocated opportunities for training, continuing education, and skill advancement. Additionally, while healthcare professionals may be assigned to perform standard military command and staff functions, their primary mission is focused on the delivery of high-quality healthcare to Servicemembers and their families. Finally, military healthcare practitioners are required to meet the board certification and licensing requirements stipulated by civilian governing organizations, and the Services facilitate this process through various means.

While the existing career management model for cybersecurity professionals within the services provides some incentives for service, there is still much room for improvement. For example, as global dependence on information systems and cyber services grows, the actions executed by our offensive and defensive cyber warriors will have greater potential consequences. Consider, for example, how the tactical actions executed by a government cyber operator will increasingly have strategic implications that can impact critical infrastructure, military readiness, and human lives. However, in spite of that operator's specialized skills, training and increasing scope of responsibility, he/she may be compensated at a very low level as is currently typical for our enlisted servicemembers. If that operator wishes to seek greater compensation and transition to become a commissioned officer, he/she risks losing his/her technical skills by moving to an evaluation and personnel management system focused on leadership/supervisory roles and developmental positions. In contrast, while Service physicians sometimes perform administrative or supervisory functions, their primary valuation and compensation is a function of their medical skill set.

The Services should consider adopting a recruitment, retention, and professional development model for their cybersecurity warriors that mirrors the existing model for healthcare professionals. There are many similarities between the current healthcare and cybersecurity paradigm. Cybersecurity is currently a high-demand/low-density field, making it difficult for the Services to recruit and retain skilled professionals in the face of higher salaries and competitive incentives in the private sector. Like the healthcare profession, cybersecurity is a rapidly evolving field that requires its practitioners to remain current on emerging technologies, tactics, and standards. Like the medical field, there are various categories of specialization and professional qualification for the cybersecurity workforce. Finally, the healthcare model exemplifies how the services can better integrate skilled cybersecurity professionals from the private sector via service in the Reserve component.

Recommendations:

1. *(Government)* Leverage lessons learned and best practices from personnel management programs for military healthcare professionals to help improve the recruitment, retention, and career management for uniformed cybersecurity practitioners.
2. *(Government)* Continue to define cybersecurity workforce roles, responsibilities, and education level, and training requirements along the lines of DoD 8570-1.
3. *(Government/Private Sector/Academia)* Undertake a cooperative approach among universities, cybersecurity education and certification organizations such as $(ISC)^2$, ISACA, and SANS, and government workforce management organizations to build a universally-accepted credentialing and certification process for cybersecurity specialties and workforce roles.
4. *(Government)* Close the salary gap between civilian cybersecurity professionals and their Service counterparts via incentive pays, skill pays, and retention bonuses.
5. *(Government)* Reassess current criteria describing the skill, experience, education requirements, and levels of responsibility for uniformed cybersecurity practitioners. Consider transitioning billets to officer and/or warrant officer, and consider managing cyber officers under a different evaluation and rating schema that focuses on technical skills, knowledge, and performance

rather than traditional supervisory/development roles.

6. *(Government)* Streamline the process by which skilled cybersecurity professionals are recruited and accessed in to government and military service. Revamp the criteria for direct commissioning and/or civilian grade determination based on new skill and professional development models.
7. *(Government)* Develop programs to allow skilled civilian cybersecurity professionals to be accessed into the Reserve Component in a similar manner to healthcare professionals. Allow members of the Reserves and National Guard to perform operational cybersecurity missions during drill weekends and annual training.

9. Embrace the Modern Work Culture for Hackers and Technology Professionals

Related Topic: *Cybersecurity Workforce*

Focus Area: *Government*

Discussion: Unfortunately, many government organizations (and industry contractors supporting government organizations) still embrace the antiquated "warm bodies in seats" approach to filling workforce roles. This approach values the employee reliably arriving at work with a professional appearance and performing a minimum set of job functions for a fixed number of hours per day. Under that model, an employee who unfailingly shows up well-attired to work each day and spends half the day gossiping or surfing the Internet may receive a higher performance evaluation than an employee who shows up late or leaves early but produces twice the amount of output. This approach is ill-suited for today's society, and is especially antagonistic to attracting and retaining skilled tech professionals. While there is no such thing as an "average hacker," you may be able to at least arrive at a reasonable quorum if you asked a group of experienced professionals at DefCon how to describe what might entice them to consider working for the government. A representative response might be as follows:

1. *Innovation and Entrepreneurship*. One of the things that attracted me to the technology field is solving puzzles and finding new ways to do things. I know my job description (or Statement of Work) says I am supposed to do X, but if I've got a strong handle on the "by the book" way of doing X, why not let me experiment with Y and Z in order to explore some new ways to think about X?
2. *Interesting and Meaningful Work*. I want to know that the work I'm doing somehow makes a difference, whether in advancing technology, improving national security, improving people's lives, or is somehow useful.
3. *Flexible Work Hours*. Having some control over my time is important to me. If I'm up late coding or fuzzing for vulnerability research, I may want to roll into work a few hours late or cut our early the next day. Sure, I can work around important meetings and customer engagements, but if there's nothing going on what's the harm in having a bit of flexibility in my hours as long as I am consistently a high performer?
4. *Unlimited Vacation*. I enjoy my work and want to see my organization succeed. I'm a "work hard, play hard" kind of person, so you can expect me to go the extra mile and take ownership of my share of the workload, which I enjoy doing because it is meaningful and innovative. In return, when there's a lull in the OPTEMPO that allows me to finally take my epic 3 week backpacking trip to Patagonia (or just binge-watching Star Wars for 3 weeks), I don't want to have to worry about counting up vacation hours. Realistically since I care about the mission I'll feel guilty about being gone for that long and cut my vacation to a week anyway.
5. *Relaxed Dress Code*. I am able to dress nicely for work if needed, but for the most part I feel much more comfortable in jeans, a t-shirt, and a hoodie. Since you hired me for my skills and contribution to the organization's cybersecurity posture, is what I wear to work on a daily basis

really that important?

6. *Snacks.* Hackers, developers, and geeks of all shapes and sizes run on snacks, so how about budgeting for a snack bar in the workplace? This is somewhat tongue-in-cheek, but from a practical perspective, the Government should consider the cost and potential benefits of integrating these type of perks of the modern workplace.

Organizations can think of this as a partnering approach, whereby they can tolerate certain deviations from the "norm" in exchange for a motivated, hardworking, and skilled employee. Government organizations face challenges to moving in this direction; indeed, in many cases operational and security requirements can make things like flexible hours and work-from home arrangements difficult if not impossible. However, rather than an all-or-nothing approach, organizations facing such constraints should consider innovative ways to help improve employees' work-life balance or otherwise attract nonstandard personnel. Additionally, a gradual approach whereby such flexible arrangements are offered as an incentive for good performance and demonstrated maturity may be preferable to some organizations.

Recommendations:

1. *(Academia)* Continue to assess the impact of nonstandard and innovative workplace practices on employee productivity, motivation, retention, etc.
2. *(Private Sector)* Share lessons learned and best practices to assist government organizations to accommodate flexible hours, remote work, unlimited vacation, relaxed appearance, etc.
3. *(Government)* Determine appropriate ways to incorporate aspects of modern work culture into government missions.
4. *(Government)* Continue to shift the focus towards building a productive and motivated workforce focused on output and mission impact and away from the antiquated "filling seats" approach.

10. Cybersecurity Workforce (General Recommendations)

Related Topics: *Cybersecurity Workforce, Public Awareness and Education*

Focus Area: *Government*

Discussion: The nation's cybersecurity workforce will increasingly become a strategic differentiator in protecting national security interests, securing critical infrastructure, and allowing our nation to remain competitive in the world economy. Accordingly, the government needs to prioritize the growth and education of our skilled cybersecurity practitioners. In addition to the workforce-centric recommendations already discussed, here are a few general recommendations for building and maturing a cadre of cybersecurity professionals in this country.

Recommendations:

1. *(Government/Academia)* Expand existing cybersecurity scholarship programs and consider developing new programs. Evaluate the potential for non-traditional scholarships and training opportunities, such as receiving reimbursement for completing a cybersecurity or information assurance certification.
2. *(Government/Academia)* Develop a tiered model for assessing the cybersecurity workforce. The first tier should be an aptitude-based model (such as the ASVAB or DLAB within the DoD), whereby individuals are assessed for general aptitude for a cybersecurity or technology curriculum. The second tier should be an assessment model, whereby individuals are assessed on their foundational knowledge of cybersecurity or technology concepts (similar to the MCAT for medical school) to assess their suitability for advanced training.
3. *(Government/Academia)* Integrate cybersecurity into existing core technology curriculum. At a very basic level, as soon as students begin to understand how an information system works, they should start understanding the need for and methods for securing and exploiting that

system.

4. *(Government/Academia)* Expand cybersecurity competitions. Envision a world where high school students compete against each other in capture the flag (CTF) or other similar competitions and receive the same level of support and funding as sports teams currently do.

Context: Author is currently a cyber subject matter analyst supporting a DoD joint test contract. Author has over 12 years of experience performing intelligence and information operations missions in the Active Army, Reserves, and National Guard. Author has over 7 years of experience in cybersecurity, including network and systems administration, security as a service, security consulting and assessments, and incorporating security into the systems development lifecycle. Author has performed cybersecurity functions supporting various sized organizations across multiple industry segments, including the DoD, SMBs, nonprofits, and Fortune 500 companies. Author holds a Master of Science Degree in Computer Information Systems from Boston University (2009) and Bachelor of Science Degree in Political Science from the United States Military Academy (2004).

References:

[Mor2016] *Morning Edition.* "NSA Director Rogers on DNC Hacking, Cyberwarfare and ISIS." Hosted by David Greene. National Public Radio, August 2, 2016.

[UL2016] "UL Launches Cybersecurity Assurance Program." Underwriters Laboratories, Inc., 5 April 2016. Available from http://www.ul.com/newsroom/pressreleases/ul-launches-cybersecurity assurance-program/.