EO 13636 and PPD-21
The Way Forward

August 2014

Produced by the Washington Cyber Roundtable,
with support from:

Aveshka
CALIBRE Systems
Cooley LLP
Halfaker and Associates
Lookingglass
Raytheon
SRA International

TABLE OF CONTENTS

TABLE OF CONTENTS 1

ABOUT THIS REPORT 1

I | EXECUTIVE SUMMARY 2

II | BACKGROUND 3

III | ANALYSIS 4

IV | CONTRIBUTORS 7

ABOUT WCR 9

ABOUT THIS REPORT

This report presents industry perspectives on the way forward for two major cybersecurity directives issued by the Obama Administration last year: Executive Order (EO) 13636 and Presidential Policy Directive (PPD) 21. The Department of Homeland Security can use the recommendations in this report to promote participation in the Critical Infrastructure Cyber Community (C^3) Voluntary Program that it established in February of this year.

The Washington Cyber Roundtable (WCR) prepared the report with the assistance of cybersecurity experts from Aveshka, CALIBRE Systems, Cooley LLP, Halfaker and Associates, Lookingglass, Raytheon, and SRA International.

This report is organized into four sections:

- Section I [Executive Summary] articulates the main conclusions of this report;
- Section II [Background] provides context about EO 13636, PPD-21, and the resulting Cybersecurity Framework and Voluntary Program;
- Section III [Analysis] presents a thematically organized summary of the Washington Cyber Roundtable's findings;
- Section IV [Contributors] lists the companies that donated time and expertise to support this report, and it provides contact information for WCR personnel.

I | EXECUTIVE SUMMARY

Industry generally views the NIST Cyber Framework and the C^3 Voluntary Program as positive steps toward a secure cyberspace. However, awareness of the Framework is still limited to specific communities of interest, and DHS faces a substantial undertaking to increase private sector adoption of the Framework.

For companies that are aware of the Framework, issues like privacy and individual rights present unresolved challenges. A detailed methodology for addressing privacy concerns in early drafts of the Framework was ultimately replaced by a more general and permissive list of processes and activities for consideration. As adoption of the Framework increases, best practices regarding privacy will draw industry's attention.

Financial (and other) incentives will play an important role in expanding participation in the C^3 Voluntary Program. But the most significant near-term challenge is the inability for a business to validate its adoption of the Framework. Until independent third-party mechanisms are established, DHS should consider developing a simple adoption guide to accompany the Framework and then market that guide aggressively to the private sector.

II | BACKGROUND

In February 2013, President Obama issued Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience. Together, they directed the Executive Branch to undertake a series of measures to improve the cybersecurity posture of our nation's critical infrastructure. The cornerstone of this effort was an iterative and collaborative yearlong process to develop a common structure for owners and operators of critical infrastructure to use in improving the security of their information and industrial control systems.

This effort – led by the National Institute of Standards and Technology (NIST) in concert with the Department of Homeland Security (DHS) and public, private, and non-profit stakeholders – culminated in the first iteration of the Framework for Improving Critical Infrastructure Cybersecurity ("the Framework"), which was released in February 2014. Compared to similar cybersecurity documents, the Framework is – by design – relatively simple and therefore broadly accessible. It eschews a one-size-fits-all approach, recognizing that business needs vary substantially in terms of cyber risk and therefore security requirements. As a result, the Framework enables any organization – regardless of size or industry – to determine its risk tolerance, identify its current risk level, and design a program to meet its target risk level.

Concurrent with the release of the Framework, DHS formally announced the establishment of the Critical Infrastructure Cyber Community (C^3) Voluntary Program. Also mandated by EO 13636, the C^3 Voluntary Program helps stakeholders use the Framework; conducts outreach to increase awareness of the Framework; and receives feedback from stakeholders about the Framework. With thousands of critical infrastructure facilities throughout the United States, DHS faces substantial challenges in implementing the C^3 Voluntary Program and achieving widespread use of the Framework.

This report will provide an independent, private sector perspective on ways that DHS can achieve the goals of the C^3 Voluntary Program.

III | ANALYSIS

Perspectives on the Framework itself

The Framework is a welcome step in the right direction

Industry reactions, particularly among the cybersecurity community, to the concept of the Framework are largely positive. NIST's approach to industry collaboration and iterative development were particularly well received. Most importantly, the substance of the Framework is sound. Now, cybersecurity providers can focus their clients' attention on a single, vetted, "best-of-breed" construct, as opposed to a set of standards that meet specific objectives (and only those objectives). For businesses in highly regulated industries, the Framework is often consistent with existing approaches, meaning that the effort required to use the Framework is limited. Additionally, these companies – which are at the forefront of cybersecurity capability in the private sector – now share a concept of security with less mature businesses.

The Framework is not a priority (unless regulations make it one)

Generally resistant to new regulations, industry has welcomed the voluntary nature of the Framework. However, the absence of a regulatory component may inhibit widespread adoption, primarily because businesses still have other regulations with which they must comply. When faced with the choice of investing in required standards or a voluntary Framework, they will always choose the requirements. Businesses still view the Framework as additive and not a replacement for established processes. To that end, many chief information officers (CIOs) view the Framework as another tool in their toolset, but not as an organizational priority.

With no easy way to prove Framework adoption, businesses won't embrace it

Perhaps more critically, companies do not know how to prove their use of (or "operationalize") the Framework. In the information technology sector, certifications or appraisals have long provided an incentive for businesses to invest time and resources in adopting a particular concept. Most organizations understand that the business value of embracing the Framework is in the Framework itself, not in a certification process. But they still need a way to demonstrate to customers that they are using the Framework. With no third-party mechanism to verify or validate adoption of the Framework, even Framework proponents will have difficulty making the internal business case to apply time and resources.

Over the course of 2014, some organizations have started to consider when and how the Framework might be adopted. But even though some industry stakeholders are beginning to pay attention, developing an adoption mechanism is not yet a high priority.

Incentivizing participation in the C^3 Voluntary Program

Tax breaks and financial incentives

The return on investment (ROI) in cybersecurity is notoriously challenging for businesses to quantify. This is especially true for small and medium-size businesses that – even if they appreciate the business value of enhanced cybersecurity – do not have the resources to implement a robust monitoring program to assess their cybersecurity posture. However, ROI is the primary decision-making factor for executives – if a CIO cannot articulate the financial value of participating in the C^3 Voluntary Program, then she faces an uphill battle with her peers in the C-Suite. To address this, many businesses move quickly to the concept of tax breaks or other financial incentives because they are readily quantifiable.

However, implementation of a financial incentive structure could quickly become complex or lead to market distortions, as the Department of the Treasury indicated in a preliminary report on the issue in 2013.[1] It would underscore the need to implement an independent mechanism for verification and validation of Framework adoption. And if the tax structure incentivizes businesses to invest more in cybersecurity than is necessary, it would undermine the spirit of the Framework, which allows a business to adopt a lower cybersecurity posture if it assesses its risk tolerance to be high.

Liability protections

When it comes to cybersecurity, businesses remain deeply concerned about liability. On the one hand, companies worry that their clients or third parties might bring legal action against them if hackers steal their data. On the other hand, they are concerned that sharing cybersecurity information might expose their own confidential data, leading to litigation or reputational damage. Congress has pursued legislation that would shield (from both civil and criminal liability) organizations that share cyber threat information in good faith and according to specific terms, but achieving a workable solution has proven difficult. Nevertheless, connecting adoption of the Framework as a standard of cyber hygiene with some degree of liability protection would be a strong incentive for businesses to participate in the C^3 Voluntary Program.

Privacy concerns

Concerns about privacy and individual rights present challenges to industry adoption of the Framework. Early public drafts of the Framework substantially addressed privacy; they included a multi-category "Methodology to Protect Privacy and Civil Liberties." However, in v1.0 of the Framework, the appendix was replaced by a more general (and permissive) set of "processes and activities" that organizations can consider "to address the…privacy and civil liberties implications" of Framework adoption. Whereas the earlier versions contained language such as "should identify" and "should implement", v1.0 indicates that "organizations may consider how, in circumstances where such measures are appropriate, their cybersecurity program might incorporate privacy principles." Without tactical recommendations provided by the Framework itself, industry will be paying attention to privacy best practices generated by early adopters.

Certification

Industry generally views certification as a good idea. As the Framework gains currency, the business value of Framework adoption will become more readily apparent to executives. As a "seal of cyber hygiene," Framework adoption would engender trust among a business's client base. It could also lead to competitive advantages for businesses, especially those that provide cybersecurity or information technology services.

The challenge is how to structure a certification mechanism. Companies could certify themselves, but this would lead to inconsistencies and diminish the value of the certification. Third parties could provide the certification mechanisms, but businesses aren't yet incentivized to pay for certification. Finally, the Government could set up an independent audit board to prove adoption of the Framework. This would be a consistent and impartial mechanism that could double as an

[1] "Treasury Department Report to the President on Cybersecurity Incentives Pursuant to Executive Order 13636." Retrieved from http://www.treasury.gov/press-center/Documents/Supporting Analysis Treasury Report to the President on Cybersecurity Incentives_FINAL.pdf

enforcement body if adoption of the Framework is ever required for certain businesses (e.g., those that do business with the Federal Government).

In the near term, DHS could develop an adoption guide that would allow companies to certify themselves. Combined with an aggressive outreach program, this adoption guide would increase awareness of the Framework, underscore that the investment in adopting the Framework is limited, and set the foundation for third-party certifiers should they come into being.

IV | Contributors

The Washington Cyber Roundtable thanks the following firms for volunteering their time and effort to develop this report. The insights and feedback of their technical representatives shaped the content presented in this document. This report represents the analysis of WCR. It does not necessarily imply an official endorsement from any of the contributing firms.

Aveshka

Aveshka delivers solutions and services to government and commercial customers in the areas of cyber and IT; intelligence and analytics; and policy and strategy. Aveshka's expert staff delivers focused consulting and complex solutions to address its clients' most mission-critical requirements. A woman-owned small business, Aveshka is recognized for thought leadership, candid advice, customer service orientation and value-driven outcomes.

CALIBRE Systems

Founded in 1989, CALIBRE Systems is an employee-owned management consulting and technology services company supporting government and industry. CALIBRE is committed to the success of its customers, and delivers enduring solutions that solve management, technology, and program challenges.

Cooley LLP

Cooley's attorneys solve legal issues for entrepreneurs, investors, financial institutions and established companies. Clients partner with Cooley on transformative deals, complex IP and regulatory matters, and bet-the-company litigation, often where innovation meets the law. Cooley has more than 750 lawyers across 11 offices in the United States and China.

Halfaker and Associates

Halfaker creates innovative and practical technology solutions in the areas of Advanced Analytics, Software Engineering, IT Infrastructure and Cyber Security to help government organizations perform their critical missions. Halfaker Information Security experts aid their clients in defending their data, information systems, and personnel against continuous and emerging cyber-attacks that pose a threat to our nation, including opportunistic hacking, insider threats, and Advanced Persistent Threats (APTs). Halfaker helps clients implement enterprise-wide security practices including, but not limited to: Security Controls Assessment (SCA) preparation and execution; Management and Operations (M&O) assessment; security technical requirements gap analysis; security technical training; IT system security analysis design and implementation. Halfaker is proud to be a service-disabled veteran-owned, woman-owned, 8(a), small business.

Lookingglass

Lookingglass provides Global Threat Intelligence Monitoring and Management to large global enterprises and government organizations. This capability is delivered through two offerings, CloudScout and ScoutVision. CloudScout provides customers with a software-as-a-service offering, while ScoutVision provides an on-premise solution enabling customers to further extend the capability into existing systems and information sets.

Raytheon

Raytheon Company, with 2013 sales of $24 billion and 63,000 employees worldwide, is a technology and innovation leader specializing in defense, security and civil markets throughout the world. With a history of innovation spanning 92 years, Raytheon provides state-of-the-art electronics, mission systems integration and other capabilities in the areas of sensing; effects; and command, control, communications and intelligence systems, as well as cyber security and a broad range of mission support services. Raytheon is headquartered in Waltham, Mass.

SRA International

For more than 30 years, SRA International has been dedicated to solving complex mission and efficiency challenges for the U.S. government. From its headquarters in Fairfax, VA, and from offices and locations around the globe, SRA's approximately 5,500 employees support government clients in defense, intelligence, law enforcement, homeland security, health and civilian agencies by delivering IT solutions and professional services in such areas as information technology lifecycle services; cloud and mobile computing; cyber security; solutions development and integration; and strategy development and organizational change management. SRA also provides mission-specific domain expertise in areas such as energy and environmental consulting; intelligence analysis; advanced research; and bioinformatics. SRA employees' deep commitment to offering real value to our clients and serving our communities is rooted in our ethic of Honesty and Service®.

ABOUT WCR

The Washington Cyber Roundtable is a non-profit, 501c(6) industry liaison group comprising a cross-section of technology, consulting, and professional services firms engaged with and affected by cyber issues. An independent, executive-level organization, WCR provides a venue for identifying research, development, and deployment priorities; disseminating best practices and lessons learned; and enhancing the cybersecurity posture of the public sector. Through focused, intimate discussions, WCR members share their business and technical expertise with government leaders to address the most complex cyber challenges facing our nation.

Contact Information

For more information about this report, please contact:

Daniel Spector
Director of Planning and Engagement
spector@washingtoncyber.org

Kaitlin Bulavinetz
Director of Operations
bulavinetz@washingtoncyber.org