ALSTON&BIRD LLP

CYBER ALERT

A Publication of the Security Incident Management & Response Team

WWW.ALSTONSECURITY.COM DECEMBER 16, 2013

NIST Cybersecurity Framework Part I: Understanding Its Structure and Potential Impact

By Kimberly Peretti and Lou Dennig

On October 22, 2013, the National Institute of Standards and Technology (NIST) released its Preliminary Cybersecurity Framework ("Framework"),[1] marking one of the final steps in creating the "voluntary" Framework envisioned in an Obama Administration Executive Order (EO) issued earlier this year.[2] That EO, which was designed to strengthen the cybersecurity of the United States' critical infrastructure,[3] required NIST to work with the private sector to develop a cybersecurity Framework to reduce the risks from cyber attacks. The Framework is designed to identify beneficial cybersecurity practices and create a common language for discussing those practices. While the Framework does not create new security standards, it uses existing standards to create a comprehensive approach to cybersecurity risk management that may be useful to companies with either nascent or more robust cybersecurity programs.

The comment period on the Preliminary Framework closed on December 13, 2013, and the final Framework is expected to be released in February of 2014. This article will provide an overview of the development of the Framework and its structure and content, discuss concerns with the Framework's current approach to privacy and analyze the extent to which the Framework will indeed remain "voluntary" for critical infrastructure entities. Finally, this article will discuss the broader implications of the Framework, including creation of a security standard of care and a ripple effect of applicability to non-critical infrastructure entities.

Part II of this series will identify any significant changes in the finalized version, when issued, and discuss the impact of this Framework on executives both within and outside of the IT departments of critical infrastructure entities.

---

1 http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

2 Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

3 The EO defines critical infrastructure to include any "physical or virtual" asset or system that is "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The Presidential Policy Directive related to the EO identifies the following 16 critical infrastructure sectors: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials and Waste, Transportation Systems, and Water and Wastewater Systems. (http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil).

I. Background on the Framework

A. Formation Process

A cornerstone principle of the EO was to ensure that the Framework was developed with significant input from the private sector. To that end, shortly after the EO was announced, NIST issued a Request for Information (RFI) designed to both encourage participation in the Framework development process and gather input from stakeholders on current industry risk management practices and use of guidelines or best practices in addressing cybersecurity issues. NIST received over 200 responses, many of which were lengthy, comprehensive responses that in some cases exceeded 100 pages. All responses were posted on NIST's website[4] and NIST later published an initial analysis of those responses.[5] That analysis grouped comments on similar topics together so that NIST could identify common themes, as well as identify "Initial Gaps" that needed to be addressed.

NIST then hosted a series of five workshops throughout the country[6] to continue to engage with stakeholders and receive additional input. Each workshop took place after NIST completed an important step in creating the Framework, thus allowing for a continuous dialogue with industry practitioners.[7] The final workshop was hosted on November 14 and 15, three weeks after the Preliminary Framework was released. Most sessions from these workshops can be viewed by webcast.[8] In releasing the Preliminary Framework, NIST announced that through the RFI and the workshops, it had engaged with over 3,000 individuals and organizations on cybersecurity standards, best practices and guidelines.[9] Indeed, initial private sector reaction to the Framework has applauded the process for developing the Framework in partnership with relevant stakeholders.[10]

B. The Framework Structure and Content

In his remarks releasing the Framework for public comment, NIST Director Dr. Patrick Gallagher described the Framework as "having really two major moving parts": first, the Framework is a "compendium of existing standards and best practices. These are practices that have been proven to be worthwhile in protecting IT systems from cyber threats."[11] Second, the Framework "provides a structure for using that compendium . . . it's a framework for organizing those practices and providing tools to support their use and adoption in businesses and organizations." The goal, as stated by the director, is to "turn today's best practices into common and expected practices."

---

4 (http://csrc.nist.gov/cyberframework/rfi_comments.html).

5 (http://csrc.nist.gov/cyberframework/nist-initial-analysis-of-rfi-responses.pdf).

6 These workshops took place in Dallas, Pittsburgh, Raleigh, San Diego and Washington, D.C.

7 An initial workshop discussed the EO, the second workshop took place two weeks after NIST released its initial analysis of RFI responses, the third workshop was held after NIST released an annotated outline of its draft Framework and the fourth workshop occurred soon after NIST published its draft Framework.

8 (http://www.nist.gov/itl/cybersecurity-framework-events.cfm).

9 (http://www.nist.gov/itl/cybersecurity-102213.cfm).

10 One week after the Preliminary Framework was released, President Obama met with eight CEOs from critical infrastructure organizations who commended the development process. (http://www.whitehouse.gov/the-press-office/2013/10/29/readout-president-s-meeting-ceos-cybersecurity).

11 (http://www.nist.gov/director/speeches/cybersecurity-framework-remarks-102213.cfm).

To accomplish that goal, the Framework is split into three categories: Framework Core, Framework Profile and Framework Implementation Tiers. The aptly named Framework Core is the backbone of the Framework, as it organizes cybersecurity activities (e.g., maintaining audit log records or controlling access to systems and assets) into distinct categories, and then provides a useful existing standard, guideline or best practice for each activity. The Framework Core thus allows organizations to identify the best practices associated with any cybersecurity activity and measure those best practices against their current practices. The Framework Profile is a tool for organizations to analyze their current cybersecurity practices and create a "Current Profile"; then, after conducting a risk assessment on potential cyber threats, the organization is tasked with creating an aspirational "Target Profile" that shows an improved cybersecurity posture. The Implementation Tiers allow organizations to determine how sophisticated their practices are with respect to cybersecurity and identify what Tier that organization currently, and should, fall into based on their industry position and available resources.

i. Framework Core

The Framework Core is essentially a roadmap that allows organizations across industries to uniformly organize their cybersecurity activities into distinct categories. Once those activities are categorized, the Framework provides a useful standard, guideline or common practice that organizations can look to as a benchmark for their internal practices. The Framework Core is comprised of four elements that together organize cybersecurity activities and identify best practices for each activity. Those four elements are Functions, Categories, Subcategories and Informative References.

The Framework Core first organizes cybersecurity activities into the following five high-level "Functions": Identify, Protect, Detect, Respond and Recover. Within each Function, cybersecurity activities are split into distinct Categories and are further differentiated into Subcategories. Each cybersecurity activity makes up one Subcategory in the Framework. The Framework notes that those Subcategories may be better described as "high-level outcomes," such as "Data-at-rest is protected" or "Notifications from the detection system are investigated."[12]

Potentially the most important aspect of the Framework Core is that each of those Subcategories, or outcomes, is associated with an Informative Reference, which provides a current industry best practice that organizations should look to as a benchmark for achieving the given outcome.[13] In doing so, the Framework creates a structure by which organizations can categorize their cybersecurity activities, identify current best practices and measure those practices against their current ones. The Framework Core thus allows entities to determine whether their

---

[12] (http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf).

[13] To gain a better understanding of how the Framework Core functions, it is illustrative to track how the Framework Core identifies the cybersecurity activity of properly destroying information as Subcategory "PR.IP-6: Information is destroyed according to policy and requirements." That activity falls under the overarching Function "Protect," which encompasses activities that implement appropriate safeguards to "ensure delivery of critical infrastructure services." Activities categorized under "Protect" are given the identifying prefix of "PR." The Protect Function includes six Categories, including Information Protection Processes and Procedures. Activities nested under that Category are given the additional prefix "IP." That Category includes activities that are maintained to manage the protection of information systems and assets. The sixth-listed Subcategory is "Information is destroyed according to policy and requirements"; therefore, the cybersecurity activity of information destruction is classified under the Framework Core as "PR-IP-6." The Framework Core provides three relevant "Informative References" for this Subcategory: COBIT BAI09.03, ISO/IEC 27001 9.2.6 and NIST SP 800-53 Rev 4 MP-6. Those Informative References refer to existing industry best practices that deal with information destruction. (http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf).

cybersecurity practices are meeting, exceeding or falling below best practices. Of course, organizations that currently use one of the existing five standards listed in the Informative References section[14] can more quickly determine whether they have practices in place in each of the designated Subcategories and, as a result, to what extent they may be deemed to have adopted the Framework.

In organizing cybersecurity activities in this way, the Framework Core also creates a common language for the purpose of allowing easier communication on cybersecurity issues, both among industry participants and in discussions with the government. It accomplishes that goal by specifically defining all cybersecurity activities, thereby allowing organizations and the government to easily refer to any given activity and inquire about an organization's current practices related to that activity.

ii. Framework Profile and Implementation Tiers

The remaining two sections of the Framework include the Profile and Implementation Tiers. One important purpose of the Framework is to allow organizations to create new or improved cybersecurity policies and procedures that are aligned with industry best practices. To do so, organizations are tasked with using the Framework Core to identify their "Current Profile," as well as a "Target Profile" to determine the gaps in their current cybersecurity practices.

Organizations are first to create a "Current Profile" that shows how far along their cybersecurity protections are in aligning with industry best practices for each Subcategory. After identifying a "Current Profile," those organizations are to conduct a risk assessment that analyzes the likelihood of a cyber attack and the impact such an attack could have on the entity.[15] Based on that risk assessment, critical infrastructure organizations are then to create a "Target Profile" outlining an intended cybersecurity posture. In creating a "Target Profile," organizations can identify gaps in their current practices, prioritize those gaps and determine the resources necessary to bridge them. Organizations should then create an action plan to achieve that "Target Profile" by enacting the industry best practices identified in the Informative References from the Framework Core.

The Framework also asks organizations to identify their current and target Implementation Tiers. There are four distinct Implementation Tiers that describe increasing levels of sophistication in terms of cybersecurity risk management practices, and the integration of those practices into an entity's overall risk management plan.[16]

---

[14] These references include Council on CyberSecurity Critical Security Controls (CCS CSC), Control Objectives for Information and Related Technology (COBIT), International Society of Automation (ISA) 99.02.01, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 and various NIST Special Publications (SP).

[15] This analysis should also take into account an organization's sector goals, the regulatory requirements in the industry and the organization's general risk management priorities. (http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf).

[16] Those four Tiers, in order from least comprehensive to most comprehensive, are Partial, Risk-Informed, Risk-Informed and Repeatable, and Adaptive. The Framework provides guidance on how organizations can identify what Tier they currently—and wish to—fall under. To do so, the Framework provides definitions of policies and procedures that the type of organizations that fall into each Tier should have in place in three areas: Cybersecurity Risk Management Processes, Integrated Programs and External Participation. For example, in a Tier 1 "Partial" organization, Risk Management Processes are not expected to be formalized and, at those organizations, "risk is managed in an ad hoc and sometimes reactive manner." The Risk Management Processes for a Tier 3 "Risk-Informed and Repeatable" organization are to be "formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to a changing threat and technology landscape." (http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf).

Organizations are meant to identify a desired Tier based on what is feasible and cost-effective for that organization. In doing so, organizations can better determine what resources they should devote to improving cybersecurity measures.

Of potential concern is the extent to which organizations may be required to disclose their Target Profile or their Implementation Tier to regulators (and, potentially, business partners), as the disclosure of either one or both may reveal weaknesses in an entity's current security infrastructure. Such weakness could be the basis of potential liability in the aftermath of a reportable security event or further regulatory inquiries.

iii. Concerns with the Framework's Current Approach to Privacy

The EO directs that the Framework include a methodology to protect individual privacy and civil liberties.[17] That methodology is included in an appendix to the Framework ("Privacy Appendix") and is based on the well-known principles known as the Fair Information Practice Principles (FIPPs). The eight FIPPs form the core of the Privacy Law of 1974, which governs federal agencies' information practices related to the collection and maintenance of personally identifiable information (PII) on their systems.[18] A variation of these FIPPs form the basis of the practices the Federal Trade Commission (FTC) encourages private sector entities to adopt in collecting, maintaining and using PII, particularly with respect to certain online activities.[19] Importantly, the FTC's FIPPs are only recommended practices that, while used as a basis for enforcement under § 5 of the FTC Act,[20] are not otherwise required by law. As it stands, the FIPPs referenced in the EO only create requirements for federal agencies, not private sector entities.

With the FIPPs as guiding principles, the Privacy Appendix organizes privacy and civil liberty practices using the same categorization structure as the Framework Core, thereby providing a methodology for how organizations should treat PII vis-à-vis each cybersecurity activity. In doing so, however, the Framework builds a privacy layer into a cybersecurity initiative and potentially transforms what were otherwise recommended privacy practices in the private sector into potentially enforceable practices. Obviously, the implications of this practical effect are significant.

As an additional point, because the provided methodology is based on the FIPPs, which are principles and not standards, the Framework does not identify benchmarks by which organizations can measure their privacy

---

17 Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,741 (Feb. 12, 2013).

18 The EO references the FIPPs set forth in Appendix A of the National Strategy for Trusted Identifies in Cyberspace (http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf). *See also 5 U.S.C.A. § 552a (the Privacy Act of 1974); Appendix B: Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program (*http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf). Those eight principles are Transparency, Individual Participation (seeking consent of affected individuals where practicable), Purpose Specification (articulate authority to, and purpose of, PII collection), Data Minimization, Use Limitation, Data Quality and Integrity, Security (protect PII against loss, unauthorized access or use), and Accountability and Auditing. (http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf).

19 (http://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission).

20 *See 15 U.S.C § 45 (prohibiting "unfair or deceptive acts or practices in or affecting commerce").*

practices.[21] To account for this lack of specificity, the Framework lists privacy standards as an area of needed improvement;[22] therefore, we can expect additional changes to the privacy methodology in the final Framework.

II. Is the Framework Mandatory?

Through every step in creating the Framework, NIST and the White House have, of course, been careful to note that the decision of whether to adopt the Framework is "voluntary." However, there are several structural components to the EO that are likely to compel critical infrastructure entities to adopt the Framework. First, Section 8 of the EO orders the Secretary of Homeland Security (the "Secretary") to work with sector-specific agencies to establish a voluntary program (the "Program") that supports Framework adoption.[23] As part of that Program, sector-specific agencies are tasked with providing an annual report to the President of the extent to which owners and operators are participating in the Program. To prepare the report, government agencies will need to make inquiries to private sector organizations on their degree of adoption of the Framework. Companies may naturally be hesitant to indicate either minimal or incomplete adoption, as they may fear such responses could prompt additional inquiry concerning the entity's cybersecurity practices. As such, it may be difficult for entities in receipt of such inquiries to view Framework adoption as a truly voluntary decision.

Second, Section 10 of the EO indicates that the Framework is a floor, rather than a ceiling, for critical infrastructure cybersecurity. The EO tasks sector-specific agencies to work with the Department of Homeland Security (DHS), the Office of Management and Budget and the National Security Staff to analyze the Framework and determine whether existing regulatory requirements provide sufficient protections against the cybersecurity risks contemplated in the Framework.[24] Importantly, those agencies must determine whether they have the authority to establish any necessary additional regulatory requirements or if legislative action is needed to empower the agencies to enact such regulations.[25] Section 10 indicates that if Framework adoption is not widespread enough to adequately protect against cybersecurity risks to critical infrastructure, those risks could be addressed with added regulation. Critical infrastructure entities may therefore view adopting the Framework as a means of avoiding added regulation, thus making Framework adoption a more palatable alternative.

Third, the proposed incentives for adopting the Framework may be so attractive that the costs of not adopting the Framework leave entities with just one viable option. As part of the Program for adopting the Framework set forth in Section 8, the Secretary is tasked with establishing a set of incentives to encourage organizations to adopt

---

21 The Informative References in Appendix B are all to Appendix J of NIST SP 800-53, rev. 4, concerning the "Security and Privacy Controls for Federal Information Systems and Organizations." (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf). The privacy controls in that document are all based on the FIPPs and reference the Privacy Act of 1974.

22 Because of these shortcomings, NIST requested additional input to identify best practices that could be included in the final Framework, so that organizations may assess their privacy standards, identify gaps and work to bridge those gaps. All recommended areas of improvement are listed in Appendix C to the Framework. (http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf).

23 Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed. Reg. 11,739, at 11,741 (Feb. 12, 2013).

24 The EO requires those agencies to submit a report 90 days after the Preliminary Framework is released to provide this guidance. Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,742 (Feb. 12, 2013).

25 Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,743 (Feb. 12, 2013).

the Framework.[26] As directed by the EO, the Secretaries of Commerce, Homeland Security and Treasury each submitted a report to the Administration recommending incentives.[27] The Administration distilled those reports into eight areas of potential incentives.[28] One proposed incentive was to make Framework adoption either a prerequisite or weighted criteria for receiving federal critical infrastructure grants, which may compel compliance with certain requirements. Other incentives, including access to a cybersecurity insurance market and reduced tort liability, could similarly make the costs of not adopting the Framework too high. The matter of incentives continues to be discussed by the Administration.

III. Broader Implications of the Framework

Not only are critical infrastructure entities likely to view Framework adoption as compulsory, but the Framework may also have a broader impact (and perhaps be as compulsory) on the contractors, partners and service providers to such entities. At a minimum, if sector-specific agencies are asking critical infrastructure entities about their level of Framework adoption, those entities will naturally turn to their service providers and contractors to inquire as to their level of adoption. Such a step is, in fact, contemplated by the Framework.[29] Critical infrastructure organizations can only feel assured that their cybersecurity protections are Framework "compliant" if their partners' practices are also so compliant.[30] Businesses hoping to maintain relationships with critical infrastructure entities may therefore see Framework adoption as a necessary aspect of those relationships. Contractors, partners and service providers may come to find that Framework adoption is a near prerequisite for working with critical infrastructure entities—and becomes an integral marketing tool for winning contracts.

---

[26] Improving Critical Infrastructure Cybersecurity, Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,742 (Feb. 12, 2013).

[27] The Treasury report, for example, recommended five incentives, including encouraging increased information sharing, clarifying liability risks, funding cybersecurity research, providing technical assistance and accelerating the security clearance process. That report also stated that Treasury did not support incentives related to tax breaks and a cybersecurity insurance market, because government involvement in those areas was either untenable or unnecessary. (http://www.treasury.gov/press-center/Documents/Treasury%20Report%20(Summary)%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf).

[28] Those eight incentives were access to a cybersecurity insurance market, grant preference, process preference, liability limitation, streamlined regulations, public recognition, rate recovery for price regulated industries and cybersecurity research support. (http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework); *see also* http://www.alstonprivacy.com/blog.aspx?entry=5015.

[29] One Category in the Framework Core under the Function "Protect" is "Awareness and Training," which identifies best practices for ensuring that an organization's general users, privileged users, senior executives and physical and information security personnel all understand their roles and responsibilities in terms of cybersecurity practices. That Category also includes best practices for ensuring that "third-party stakeholders (suppliers, customers, partners) understand [their] roles & responsibilities." (http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf).

[30] The U.S. Department of Defense published a final safeguarding rule that could potentially mandate contractor compliance with the Framework. (http://www.gpo.gov/fdsys/pkg/FR-2013-11-18/pdf/2013-27313.pdf). The rule requires that contractors in possession of unclassified nonpublic technical information (UCTI) satisfy the security controls found in NIST SP 800-53. If the contractor does not implement the control found in that document, the contractor must provide a written explanation as to why that control is not applicable and/or provide an alternative measure that is in place and can be considered an "equivalent protection." The rule also states that a contractor may "[a]pply other information systems security requirements when the Contractor reasonably determines that information systems security measures, in addition to those identified in [NIST SP 800-53], may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability." It is reasonable that contractors would look to the Framework for such "equivalent protection" or to identify additional security measures necessary to "provide adequate security in a dynamic environment based on an assessed risk or vulnerability." See also http://www.alstonprivacy.com/blog.aspx?entry=5125.

The natural progression of a circle of 16 critical infrastructure industries and their contractors, partners and service providers adopting the Framework is that such adoption will extend to those entities' noncritical infrastructure business relationships as well. In engaging in general business relationships, such as marketing and the provision of basic services, critical infrastructure entities may inquire about the cybersecurity practices those organizations have in place. Noncritical infrastructure entities hoping to provide adequate responses to such inquiries may themselves be compelled to adopt the Framework. Even though Framework adoption is supposed to be voluntary for critical infrastructure entities, it is not difficult to see the ripple effect the Framework may have, over time, of creating the standard by which businesses judge one another's cybersecurity practices.

Use of the Framework as the standard by which an organization's cybersecurity practices are measured could occur in two ways: (1) the entity, regardless of whether it is involved in critical infrastructure, adopts the Framework; or (2) the Framework becomes the de facto standard because it was developed by the government working in close consultation with the private sector, thus giving the industry best practices highlighted in the Framework an aura of legitimacy. Use of the Framework as a de facto standard is especially likely if the Framework becomes widely adopted. Even if the Framework does not gain widespread acceptance and use, the practices in the Framework could nonetheless be looked to as the standard by which to measure an organization's practices. This could have the significant effect of creating a standard of care for use in establishing legal liability. Having such a standard in place has benefits and drawbacks: while it creates certainty for organizations looking to protect themselves from liability, it also holds organizations to a standard they may not wish to meet due to the costs of compliance or based on an internal risk assessment.

Critical infrastructure entities that have business relationships with those organizations should closely monitor the creation of the final Framework, as it is likely to be a key component of cybersecurity discussions and practices for the foreseeable future.

Security Incident Management & Response Team Co-Chairs
Kim Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com
www.alstonsecurity.com