dentons.com

DENTONS

Insights and Commentary from Dentons

The combination of Dentons US and McKenna Long & Aldridge offers our clients access to 1,100 lawyers and professionals in 21 US locations. Clients inside the US benefit from unrivaled access to markets around the world, and international clients benefit from increased strength and reach across the US.

This document was authored by representatives of McKenna Long & Aldridge prior to our combination's launch and continues to be offered to provide our clients with the information they need to do business in an increasingly complex, interconnected and competitive marketplace.

Bloomberg BNA

Federal Contracts Report™

Framework As Foundation: How Government Contractors Can Use the NIST Cybersecurity Framework




BY ELIZABETH A. FERRELL, PHILLIP R. SECKMAN, ERIN B. SHEPPARD, MICHAEL J. MCGUINN

Nearly two months after the release of Version 1.0 of the National Institute of Standards and Technology's (''NIST'') Cybersecurity Framework (the ''Framework''), many government contractors are still considering how, if at all, to use the Framework in their own day-to-day operations. That industry is proceeding with some caution is understandable. For contractors with mature cybersecurity regimes in place, the Framework may do nothing more than confirm the sufficiency's existing approach. For other contractors considering how to roll-out or improve cybersecurity practices, adopting a compliance regime on par with the Framework may seem unattainable or extremely costly, with minimal incentives for early adopters.

The Framework ultimately may not be for everyone. But contractors who entirely ignore the Framework risk missing out on a potentially valuable tool to integrate cybersecurity and cyber risk management into their organizations. This second article in the Federal Contracts Report's series on cybersecurity will help contractors better understand how they can make the Framework work for them. It will discuss the Framework's background, its applicability for to government contractors, including non-critical infrastructure providers, and provide important practical considerations and key takeaways for companies still grappling with the question of how best to utilize the Framework tool kit.

Elizabeth Ferrell (eferrell@mckennalong.com) and Phillip R. Seckman (pseckman@mckennalong.com) are partners in McKenna Long & Aldridge LLP's government contracts practice. Erin B. Sheppard (esheppard@mckennalong.com) and Michael J. McGuinn (mjmcguinn@mckennalong.com) are associates in the firm's government contracts practice.

I. Background. Version 1.0 of the Cybersecurity Framework, released in February 2014, is the culmination of a year-long initiative.. In February 2013, President Obama issued Executive Order 13636[1] (the ''EO'') and the corresponding Presidential Policy Directive on Critical Infrastructure Security and Resilience (the ''Directive''). The EO and Directive launched a multi-step collaboration between the public and private sectors to develop and refine a uniform set of cybersecurity standards and corresponding tools.

The EO mandated, among other things, that NIST coordinate and develop a framework to reduce cyber risk to critical infrastructure. Specifically, the EO directed NIST to create a framework that incorporated a set of standards, methodologies, procedures, and processes to assist in aligning policy, business, and technological approaches to addressing cyber risk.

NIST held more than five workshops, as well as multiple meetings and information sessions with industry and other key stakeholders over the course of its year-long framework drafting and refinement process. In October 2013, NIST issued a preliminary framework and solicited public comments. More than 200 commenters filed comments in response; many of which addressed

[1] Executive Order 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013).

 ISSN 0014-9063

privacy, cost-effectiveness, or other similar industry concerns. Version 1.0 of the Framework incorporated certain suggestions, but others — including the various comments regarding the lack of concrete incentives and discussion regarding cost effectiveness discussed further below — remained largely unanswered.

II. Reaction from Industry. The public reaction since the release of Version 1.0 of the Cybersecurity Framework has been positive, albeit somewhat divided. Though many laud the structure of the Framework and the flexible approach contained therein, others question whether the voluntary and abstract nature of the Framework's guidance will ultimately detract from voluntary adoption of the Framework itself. Likewise, others have bemoaned the lack of any specific incentives to bolster the likelihood that a particular entity will adopt the Framework. Still others — and government contractors in particular — are left wondering what the expectation is for adoption of the Framework outside of critical infrastructure sectors. This section provides a brief summary of these issues.

A. Framework Incentives. Section 8(d) of the EO called upon the Departments of Homeland Security, Commerce, and Treasury to suggest incentives for adoption of the Cybersecurity Framework. Those departments issued a report in which they outlined various policy options and identified specific incentives that merited further consideration by the administration following issuance of the Cybersecurity Framework.[2]

As described by the administration in August 2013, the various incentives under consideration at that time included: (1) making cybersecurity insurance available for adopters of the Framework; (2) inclusion of participation in the voluntary framework as an eligibility factor for federal critical infrastructure grants; (3) providing preference to voluntary participants in a range of technical assistance programs; (4) limiting liability for tort, indemnification, and state law disclosure requirements; (5) creation of public recognition programs for adopters; (6) rate recovery for price regulated industries; (7) cybersecurity research; and (8) streamlining existing regulations.[3]

Much to the disappointment of those looking for strong incentives to encourage adoption, Version 1.0 of the Framework did not include any discussion of these potential incentive mechanisms.[4] The Administration has stated that incentives are still under review and do not expect any specific action in the early stages of the Framework's release.[5] Some organizations, such as the Information Technology Industry Council, think preventing damage caused by cyber-attacks ought to be incentive enough for entities confronting such challenges and have publicly recommended de-emphasizing a short-term push for incentives in favor of a longer-term approach.[6] The failure to include such incentives raises the question of whether contractors should anticipate such incentives in the future.[7] The lack of concrete answers may lead some companies to adopt a wait-and-see approach, rather than take any specific actions to voluntarily implement the Framework at this time.

B. Framework Cost-Effectiveness. Part of NIST's mandate under the EO was to ensure that the Cybersecurity Framework, in addition to being flexible, repeatable, and performance-based, was also cost-effective.[8] Despite this mandate, however, certain industry groups have bemoaned the administration's failure to consider this practical aspect of individual companies' risk assessments when issuing the version 1.0 of the Framework. The Internet Security Alliance (''ISA'') issued a report in early February criticizing NIST's failure to provide any guidance for owners and operators on how to assess the utility of the Framework from a cost-effectiveness standpoint.[9] In its paper, the ISA noted that without data or analysis regarding the cost effectiveness of potential implementation of the Cybersecurity Framework, industry will have tremendous difficulty assessing whether or not to voluntarily adopt the Framework.

C. Standards of Care. Finally, there is some disagreement over whether the Framework has the potential to become a *de facto* standard of care for corporations concerned with protecting against cyber threats. Some have opined that plaintiffs lawyers may rely heavily upon the Framework in the event of a cyber incident by characterizing the Framework as a collection of the measures companies should have adopted or considered in order to prevent misappropriation of sensitive information, such as financial or trade secret data. The Congressional Research Service picked up on this suggestion in a legal sidebar provided to House and Senate offices in early March.[10]

Others are more skeptical about the Framework's likely role in such litigation. For example, varying state law interpretations as well as the inherent flexibility

---

[2] Michael Daniel, *Incentives to Support Adoption of the Cybersecurity Framework*, The White House Blog (Aug. 6, 2013), available at http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

[3] *Id.*

[4] *See, e.g.* Eric Chabrow, *Incentivizing the Cybersecurity Framework: Getting Industry to Adopt the Recommended Best Practices*, GovInfoSecurity (Feb. 18, 2014) available at http://www.govinfosecurity.com/incentivizing-cybersecurity-framework-a-6510/op-1.

[5] *See* Charlie Mitchell, *Technology group downplays incentives in recommendations on DHS Voluntary Program*, Inside Cybersecurity Daily News (Feb. 11, 2014), available at http://insidecybersecurity.com/Cyber-Daily-News/Daily-News/technology-group-downplays-incentives-in-recommendations-on-dhs-voluntary-program/menu-id-1075.html.

[6] Information Technology Industry Council, *ITI Recommendations to the Department of Homeland Security Regarding its Work Developing a Voluntary Program Under Executive Order 13636, ''Improving Critical Infrastructure Cybersecurity''* (Feb. 11, 2014), available at www.itic.org/. . ./3ed86a62-b229-4d43-a12b-766012da4b1f.pdf.

[7] *See, e.g.*, Dietrich Knauth, *Cybersecurity Framework Previews Contracting Changes*, Law360.com (Feb. 18, 2014), available at www.law360.com/articles/510217.

[8] E.O. 13636, § 7(b).

[9] *Internet Security Alliance: Framework fails to meet 'cost-effective' mandate*, Inside Cybersecurity Daily News (Feb. 5, 2014), available at http://insidecybersecurity.com/Cyber-Daily-News/Daily-Briefs/internet-security-alliance-framework-fails-to-meet-cost-effective-mandate/menu-id-1075.html

[10] Nancy Oganovich, *Congress Told New Cybersecurity Plan from NIST Raises Liability Issues*, BNA Federal Contracts Report (March 7, 2014), available at http://news.bna.com/fcln/FCLNWB/split_display.adp?fedfid=42726327&vname=fcrnotallissues&wsn=500340000&searchid=22410709&doctypeid=1&type=date&mode=doc&split=0&scm=FCLNWB&pg=0

  FCR ISSN 0014-9063

within the Framework may militate against a pressing concern that the Framework will be applied in such a uniform, liability inducing fashion.[11] The same uncertainties about how to ''adopt'' the Framework could make it tremendously difficult for a court to adopt the web of functions and guidance as a de facto industry standard of care.

III. Practical Guidance for Government Contractors. Contractors considering how to use the Framework should carefully consider and monitor the foregoing issues, as resolution of these concerns will impact whether and when to use the Framework. Even absent resolution, the Framework remains a potentially useful tool for contractors grappling with cybersecurity compliance and existing threats. As we explained in our initial piece in this series, the Framework's processes, procedures, and organizational constructs, although developed for critical infrastructure providers, are useful for a much broader audience. This includes government contractors, large and small, at all levels of the supply chain.

The Framework's primary benefit is its flexibility. The Framework, in large part, is a process for managing cyber risk. Because different companies face different risks and have different levels of cybersecurity sophistication, ''adoption'' will mean different things to different companies. The Framework recognizes this reality, provides no definition of ''adoption'' and purposefully avoids one-size-fits-all ''check the box'' solutions. Indeed, contractors already facing the burden of complying with the DFARS clause on safeguarding unclassified technical information (''UCTI'') are all-too-familiar with the potential difficulties associated with these types of seemingly inflexible security controls (where they do not have equivalent protections in place). By avoiding this approach, the Framework allows companies to develop tailored solutions based on each individual company's actual cyber risks. And importantly for contractors, it also provides flexibility to balance these risks against the costs of implementation..

Consistent with this benefit, the precise application of the Framework will vary depending upon the current state of a contractor's cybersecurity program. Contractors with non-existent or more rudimentary programs likely stand to gain more from of the Framework's principles. Yet, the Framework also provides a unique opportunity for more sophisticated contractors to review existing cybersecurity programs through a fresh lens. No matter how robust an existing organization's cybersecurity program may be, the Framework contains certain additional benefits that such contractors may want to review and consider utilizing. For example, organizations with detailed cybersecurity policies and procedures may nevertheless be able to adopt the language or thematic organization of the Framework to better communicate the company's cyber needs to internal and external stakeholders. Likewise, large prime contractors could also use the Framework to create a ''target'' cyber profile for higher-risk subcontracts, to serve as a prerequisite for award or as a basis of comparison among potential suppliers.

For new entrants to this area and smaller government contractors who may be just beginning to grapple with what cybersecurity threats mean to their operations, the Framework provides a ready-made, albeit complex, template for action. In particular, Section 3.2 of the Framework provides a basic list of the critical steps any entity should take when creating an effective cybersecurity plan. This is where newcomers should begin their review of the Framework.

Specifically, the Framework recommends that each organization first prioritize and scope its business/mission objectives and organizational priorities in order to guide the manner in which the entity will adopt the Framework. Second, once the contractor has reached a determination regarding the intended scope of its cybersecurity program, the contractor should then focus on identifying related systems, assets, and overall risk approach for the contractor organization. Third, the contractor should create a current profile to inventory which of the current Framework categories and subcategories have been addressed. Fourth, the Framework recommends performing a risk assessment to analyze the operational environment and determine the likelihood of a cybersecurity event. Finally, in the last three steps, the Framework recommends creating a target profile that captures the organization's desired security outcomes, analyzing the gaps between the current and target program, and implementing an action plan for closing any such gaps.

Practically speaking, a business that is conducting such an assessment for the very first time may chose to focus on a more limited number of categories and subcategories within each of the Framework's five functions: Identify, Protect, Detect, Respond, and Recover. For example, a novice in the field may choose to spend more time on the identify function so that it may better acquaint itself with the vulnerabilities of the company's existing assets and business environment. By conducting a more fulsome risk assessment and gauging the organization's tolerance for risk management, the company can be better suited to pick and choose between the categories and subcategories within each of the remaining functions. Even if a contractor is only able to perform a single subtask in each of the five functions, presumably that contractor will be better off than had it done nothing at all.

IV. Key Take-Aways. As discussed throughout this article, adoption and implementation of the Framework will occur in many vastly different manners across a range of critical infrastructure and other closely related industries. In the interest of assisting government contractors grappling with how best to use the Framework, we are providing some practical tips regarding cybersecurity program implementation using the Framework tools.

- **Start small and increase efforts from there**

For entities that are using the Framework's release as the impetus to undertake a thorough review the organization's cyber vulnerabilities, the broad and seemingly all-encompassing nature of the Framework could potentially lead to a state of paralysis. However, rather than being deterred by the Framework's lengthy compilation of standards, tentative contractors should con-

[11] *See, e.g.,* Christopher J. Castelli, *Lawyers Disagree on whether cybersecurity framework will reshape liability landscape*, Inside Cybersecurity (Feb 20, 2014), available at http://insidecybersecurity.com/Cyber-General/Cyber-Public-Content-Special-Promo/lawyers-disagree-on-whether-cybersecurity-framework-will-reshape-liability-landscape/menu-id-1105.html.

sider a more gradual approach to ''adoption'' if necessary. For example, a small contractor may choose to zero in on what it believes to be the critical subcategory activity within each of the function categories. Selecting a smaller subset of subcategories in each function to focus on will provide a foundation for more comprehensive action down the road if necessary.

■ **Utilize the Framework to Facilitate Compliance with the New DFARS Clause Regarding UCTI**

While the various implementation issues that arise under the new DFARS Clause (252.204-7012) will be addressed in the next article in this series, contractors should recognize the potential benefits of utilizing the Framework as a tool to assist in achieving compliance. The Framework, by design, provides understandable and common terminology to enable effective communication between all personnel with a role in achieving and monitoring compliance and security of the company's information system. Additionally, contractors should anticipate that some portion of the Framework, while voluntary today, may become mandatory in the future. Thus, investing in adopting the Framework while it is voluntary enables companies to deal with the Framework on their terms rather than rushing for compliance after they have been awarded a contract containing cybersecurity standards, like the DFARS clause on safeguarding unclassified controlled technical information. Contractors utilizing the Framework core, which contains many (but not all) of the same NIST security controls as those incorporated into the DFARS clause, will be better positioned to comply with the DFARS clause requirements for systems containing UCTI.

■ **Communicate strategic objectives to key internal and external stakeholders**

Given the lack of any recommended path to implementation and in light of the tremendously varied manners in which organizations may choose to use the Framework's scalable, repeatable processes, it is important for any entity that believes itself to be ''adopting'' the Framework to clearly communicate its objectives to key internal and external stakeholders. Using again the example of a small government contractor, the question of which category and/or subcategory to emphasize will depend largely upon the company's independent business priorities and the nature of the highest risk vulnerabilities for the company. Once such a decision is made, the company should be certain to clearly communicate the implementation plan both internally and externally to define what ''adoption'' will mean for the organization.

■ **Consider suppliers in the assessment equation**

In addition to reviewing the company's own individual cyber protections, government contractors should consider instituting a review of the contractor's supplier and/or subcontractor protections. This is an area that may be of greater concern for larger contractors with more complex supply chains, and, as discussed above, may be accomplished by creating target profiles for specific acquisition types. However, even smaller contractors should bear in mind the additional risk posed by such supply chain vulnerabilities. A review of supply chain protection and accountability is a clear priority for any organization providing goods or services to the government that may be subject to cyber threats. A critical component of any new cybersecurity assessment is a concrete and up-front decision for how to protect against cyber risks within the contractor's own supply chain.

■ **Remain engaged in the ongoing industry dialogue**

On the same day NIST released version 1.0 of the Framework, DHS announced the creation of the Critical Infrastructure Cyber Community — C^3 (pronounced C-cubed) — another voluntary program intended to serve as the coordination point within the Federal Government for critical infrastructure owners and operators seeking to improve cyber risk through the use of the Framework. DHS is working on developing a sectoral approach via the C-cubed initiative—so to the extent a particular contractor is heavily engaged in a single sector, monitoring developments in that sector is fundamentally important.

NIST also simultaneously issued a Roadmap for Improving Critical Infrastructure cybersecurity in which it laid out a number of additional opportunities for collaborations amongst key stakeholders and confirmed that it intends to release at least one more release of the Framework before ceding ownership of the document to DHS or another appointed entity. Remaining abreast of the continued developments in this area will allow contractors to help shape future developments and be best poised for action in response to future initiatives.

  FCR ISSN 0014-9063