Van Ness Feldman LLP

vnf.com

GAO Reports Challenges and Successes in Cybersecurity Framework Adoption

MARCH 5, 2018

Gwen Keyes Fleming, T.C. Richmond, Mike Farber, Darsh Singh, and R. Scott Nuzum

The Government Accountability Office's ("GAO") February 2018 report, entitled "Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption," outlined the progress the federal government, industry and their affiliates have made in protecting critical infrastructure. Perhaps, more importantly however, the report revealed that many of the nation's foundational public and private systems continue to face challenges in implementing coordinated efforts to secure those systems from cyber threats, save for notable progress in a few sectors. As regulators and legislators continue to explore the best methodologies of protection and dispatch resources to address the country's cyber threats, critical infrastructure entities must remain vigilant to stay current on the latest industry standards, best practices and procedures, technological advances and legal obligations. This alert summarizes the latest audit conducted by the GAO and the responses of the federal agencies to those recommendations.

Background

In February 2013, President Obama issued Executive Order (EO) 13636, entitled "Improving Critical Infrastructure Cybersecurity," which outlined an action plan for improving security for critical cyber infrastructure. The EO defined "critical infrastructure" to mean systems and assets that are 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 EO directed the National Institute of Standards and Technology ("NIST") to develop a voluntary, risk-based cybersecurity framework that would include a set of standards and best practices that could be used by organizations to help manage their cyber risk. In addition, the EO also directed certain federal agencies that work directly with critical infrastructure entities, referred to as sector-specific agencies ("SSAs"), to review the cybersecurity framework and, if necessary, develop implementation guidance or supplemental material to address sector-specific risks and identify incentives to support adoption of the Framework through a voluntary program established by the Secretary of Homeland Security. The SSAs were to report annually to the President on the level of progress made regarding the private sector's participation in the voluntary program.

As directed, NIST published the *Framework for Critical Infrastructure Cybersecurity* in February 2014 (Framework) and released an updated draft version (Framework v 1.1) in December 2017. Despite the voluntary nature, NIST and the EO intended for all critical infrastructure entities to implement the Framework in an effort to utilize the comprehensive and standardized nature of the Framework to discern cyber health on both an individual-sector and national scale.

Building on the principles contained in EO 13636, President Trump issued Executive Order 13800 "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" in May 2017 which mandated that all federal agencies use the Framework to manage their own cyber risk and provide a report outlining a plan to implement the Framework within the agency.

The GAO Study

The GAO's study, triggered by the Cybersecurity Enhancement Act of 2014, reviewed aspects of the procedures and standards developed by NIST and assessed to extent to which critical infrastructure sectors, and their associated SSAs, have adopted NIST's Framework. The GAO's study focused on sixteen critical infrastructure sectors and their nine associated SSAs, which are the Departments of: Agriculture, Defense, Energy (DOE), Health and Human Services, Homeland Security (DHS), Transportation (DOT), Treasury, General Services Administration and the Environmental Protection Agency (EPA). Most critical infrastructure sectors and SSAs have taken action to facilitate adoption of

the NIST Cybersecurity Framework by developing guidance and aligning sector information resources with the Framework's principles. Furthermore, several non-federal sector coordinating councils ("SCC") have taken additional steps to encourage framework adoption. Despite these steps, *none* of the SSAs, however, have directly assessed the extent to which their entities have actually participated in the voluntary program and *adopted* the Framework. While some SSAs have used tangential survey methods (like measuring how many Framework Tool Kits have been downloaded from a website), without reliable qualitative or quantitative measures in place, there is no way to accurately assess the degree to which the Framework has been adopted across a sector. Ultimately, this means that the federal government lacks a comprehensive methodology to measure the extent to which the critical infrastructure enterprise, either as individual sectors or comprehensively, has made progress in advancing comprehensive cybersecurity protections.

Federal agencies, which are required to implement the Framework themselves pursuant to EO 13800, indicated that the biggest challenge to determining enterprise-wide framework adoption was the voluntary nature of the NIST Framework itself and the inability of government agencies to mandate Framework implementation or even to require critical infrastructure entities to provide data related to that implementation. Several federal entities also cited regulatory obstacles, such as the Paperwork Reduction Act (44 U.S.C. §3507), which requires Office of Management and Budget approval before conducting a wide scale survey or data collection.

In addition to obstacles from the federal perspective, the study identified four other challenges to Framework adoption that were reported by the entities that were surveyed:

1. **Limited ability to commit necessary resources toward Framework adoption.** While large entities, in some cases, have larger teams and more than sufficient resources to address cybersecurity, smaller businesses in the supply chain are often unable to dedicate staff to voluntarily implement the Framework.

2. **Lack of the necessary knowledge and skills to effectively implement a Framework**. Despite efforts to introduce and promote the use of the NIST Framework by SSAs, SCCs and other federal agencies, there are still several organizations that are uncertain about whether and how to apply the Framework to their business model.

3. **Existing regulatory, industry or other requirements inhibit Framework adoption**. At least five of the sixteen sectors are heavily regulated by state, federal and sometimes local authorities; thereby creating a patchwork of overlapping, and sometimes conflicting, obligations which, in turn, creates a disincentive to voluntarily add Framework adoption to an already crowded field of priorities.

4. **Other priorities take precedence over conducting cyber-related risk management or adopting the Framework**. Due to the vast differences in size, type, function and location of critical infrastructure assets, and the resources available to protect those assets, seven SCCs indicated that companies are forced to prioritize physical security, natural disaster response and insider threats over cybersecurity. Smaller organizations are still not convinced they are a viable target for an attack, and therefore see little benefit in voluntarily adopting the Framework to address an incident with a low or zero risk of occurrence.

In light of the challenges, GAO made nine recommendations, one to each of the SSAs and their respective sector members to collaboratively "develop methods for determining the level and type of Framework adoption by entities across their respective sector." The report incorporated the responses of all nine SSAs to their respective recommendations. Five SSAs agreed with the GAO's recommendation, and the remaining four neither agreed nor disagreed.

While there seemed to be agreement with the report's findings, most entities did not identify a specific plan of action or recommendations to advance the adoption of the NIST Framework. Notably, DHS,

Van Ness Feldman LLP
vnf.com

DOE, DOT and EPA took a different approach. Specifically, DHS plans to work with the nine sectors for which the agency is an SSA to understand the barriers to adoption of the Framework and develop best practices for same by December 31, 2018. DOE committed to consulting with its sector members on the development of methods for determining the level of the Framework's adoption and also stated that, in the coming year, the agency would align its existing Capability Maturity Model (C2M2) tool with Framework v1.1. DOT indicated that an approach that calls for aggregate, non-attributional summary of Framework adoption efforts has been proposed. The EPA, as the SSA for Water and Wastewater Systems, generally agreed with the GAO's findings and conclusions but, indicated that the agency did not have the authority to activate any mechanisms to meet the desired goal. To alleviate this hurdle, EPA recommended that 1) strong mandates for the collection of information from "a federal entity with overarching responsibility for critical infrastructure cybersecurity;" and 2) the establishment of unified cross-sector metrics and methods are required in order for a survey and subsequent analysis of Framework adoption to be successful.

Looking Forward – Continuing Industry Engagement to Build Confidence and Resilience

It is universally accepted that sharing information within and across sectors, as well as with the federal government, strengthens the national fight against cyber threats. However, the absence of a legislative or regulatory mandate to implement the NIST Framework across the private sector prevents agencies from requesting information to credibly determine its level of use. Given that industry is generally opposed to any additional proscriptive regulations, there is an opportunity for non-federal SSCs, key industry-players and private-sector groups to build upon the trust already existing within the respective sectors and take the initiative to identify best practices to bolster information sharing and improve cyber health. Unlike federal agencies, these entities are not hindered by various regulatory prohibitions, appropriations limitations or mission conflicts and therefore are well positioned to continue to provide leadership in the cyber space.

The GAO has made it clear that, despite the challenges identified, it will continue to engage in audits and bring to the fore the issues and areas of deficiency with respect to broad implementation of the Framework. Some SSAs and SCCs, including DOE, the electric sector and the oil and natural gas sectors are further along the path to NIST Framework adoption than other sectors. However, even these sectors must continue to do more to reduce cyber risks, as illustrated by recent reports of illicit cryptocurrency mining by hackers at a hydroelectric facility, and a data breach by a white-hat hacker at an electric utility, which resulted in the subsequent imposition of fines by the North American Electric Reliability Corp. By creatively addressing the four challenges listed in the GAO report, these sectors are positioned to continue building their cybersecurity capabilities while serving as models for the other sectors on how best to navigate the difficulties with Framework adoption. As a demonstrated leader in self-governance, the energy sector collectively, and its electricity and oil and natural gas subgroups, can, not only strengthen the nation's cybersecurity, but also build regulator confidence in the process.

For more information

Van Ness Feldman's Cybersecurity Team is available to keep clients informed and at the forefront of cybersecurity developments. Please contact Gwen Keyes Fleming, Mike Farber, T.C. Richmond, Darsh Singh and R. Scott Nuzum at (202) 298-1800 or (206) 623-9372 if you have any questions or would like more information.

Follow us on Twitter @VanNessFeldman