CYBERSECURITY FOR GOVERNMENT CONTRACTORS—2021 UPDATES

Michael J. Vernick[1]
Akin Gump Strauss Hauer & Feld LLP

Michael J. Scheimer[2]
Hogan Lovells US LLP

I. EXECUTIVE ORDER ON IMPROVING THE NATION'S CYBERSECURITY

Among the most significant cyber-related developments in 2021 was President Biden's May 12, 2021 issuance of Executive Order (EO) 14,028 on "Improving the Nation's Cybersecurity." As noted in the Administration's accompanying Fact Sheet, the EO was a direct response to recent high-profile cybersecurity incidents (e.g., SolarWinds). It should, however, also be viewed in context as a response to years of increasing concern about, and efforts to enhance, cyber and supply chain security within the federal government, its contracting base, and the U.S. information and communications technology and services (ICTS) industry more broadly.

Building on initiatives such as Section 889, the Commerce Department's ICTS supply chain regulations, Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS) cybersecurity and incident reporting standards, and the Department of Defense's (DOD) Cybersecurity Maturity Model Certification (CMMC), among other efforts, the EO seeks to harmonize, enhance, and extend existing cyber and supply chain security requirements across the government while operationalizing several new programs and frameworks to address existing and emerging threats. We address several elements of the EO below.

A. Critical Software

Broadly, Section 4 of the EO, "Enhancing Software Supply Chain Security," seeks to establish foundational standards for the security and integrity of software products purchased by U.S. federal agencies. Of particular note is the security and integrity of so-called "critical software," which the EO broadly defined to include software that "performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources)."

The administration's focus when it comes to critical software was to advance primarily on two interrelated tracks, the first of which was to establish a definition of "critical software" and then to develop guidance for federal agencies to follow to enhance protections. To that end, the EO provided that, within 45 days of its issuance, the National Institute of Standards & Technology (NIST) was to publish a definition of the term "critical software" that will "reflect the level of privilege or access required to function, integration and dependencies with other software, direct access to networking and computing resources, performance of a function critical to trust, and potential for harm if compromised." NIST solicited position papers from the stakeholder community, hosted a virtual workshop, and consulted with the Cybersecurity and Infrastructure Security Agency (CISA), Office of Management and Budget (OMB) and others to develop a preliminary definition and initial categories of software.

On June 24, 2021, NIST released the following definition of "critical software:"

> *EO-critical software* is defined as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:
>
> - is designed to run with elevated privilege or manage privileges;
> - has direct or privileged access to networking or computing resources;

- is designed to control access to data or operational technology;
- performs a function critical to trust; or,
- operates outside of normal trust boundaries with privileged access.

The NIST publication further explained that the definition would reach software "of all forms . . . purchased for, or deployed in production systems and for operational purposes."

NIST also released a list of software that it considered "EO-critical." These include identity, credential, and access management (ICAM); operating systems, hypervisors, container environments; Web browsers; endpoint security; Network control; Network protection; Network monitoring and configuration; Operational monitoring and analysis; Remote scanning; Remote access and configuration management; and Backup/recovery and remote storage.

On July 8, 2021, NIST followed up on the critical software definition, and categories of critical software, with a series of security measures to be used in conjunction with EO-critical software. The NIST security guidance includes the following five primary objectives, each of which includes several specific security measures:

- Protect EO-critical software and EO-critical software platforms from unauthorized access and usage
- Protect the confidentiality, integrity, and availability of data used by EO-critical software and EO-critical software platforms
- Identify and maintain EO-critical software platforms and the software deployed to those platforms to protect the EO-critical software from exploitation
- Quickly detect, respond to, and recover from threats and incidents involving EO-critical software and EO-critical software platforms
- Strengthen the understanding and performance of humans' actions that foster the security of EO-critical software and EO-critical software platforms

The EO explained that after initial work was done to develop a definition of critical software, identify categories of such software, and develop security measures to protect such software, OMB would take steps to require federal agencies to comply with the new guidance. OMB did so through issuance of the August 10th Memorandum M-21-30, which provides federal agencies with instructions on how to comply with the NIST guidance. Notably, the OMB memorandum explains that agencies may follow a phased approach to achieving compliance with the NIST guidance. The memorandum provides that "[d]uring the initial implementation phase, agencies should focus on standalone, on-premise software that performs security-critical functions or poses similar significant potential for harm if compromised." Among the examples of such systems are web browsers; operating systems; and identity, credential, and access management. According to the memorandum, "[s]ubsequent phases of implementation will address additional categories of software, as determined by the Cybersecurity and Infrastructure Security Agency (CISA)."

B. Software Supply Chain Security

The EO calls for NIST to take action to improve software supply chain security. In accordance with that directive, NIST has issued two notable forms of guidance.

The first is a draft update of the "Secure Software Development Framework (SSDF) Version 1.1" that was first issued on September 30, 2021. The SSDF explains that it has two primary audiences, one is software producers (commercial and off-the shelf) and custom software developers, and the second is software purchasers and consumers (again both inside and outside the government). The September 2021 document explains that it sets forth "a set of fundamental, sound practices for secure development called the Secure Software Development Framework (SSDF)." The expectation is that the SSDF will be utilized during software development, that organizations will use the SSDF when working with third-party software suppliers, and that software developed in accordance with the SSDF will be acquired. Importantly, the SSDF is not intended to "prescribe how to implement each practice." Put another way, the SSDF is concerned with "outcomes" more than it is with how those outcomes are achieved. The SSDF explains that it takes such an approach so that it can be widely used by any "sector or community" and without regard for "size or cybersecurity sophistication." Comments on the SSDF were open through November 2021.

The second key action taken by NIST is another revision to Special Publication (SP) 800-161 Rev. 1 "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations." The initial draft of Rev. 1 of SP 800-161 was issued in April 2021, prior to EO 14,028's issuance on May 12. As was the case with the initial draft, the focus of the publication is to "provide[ ] guidance to organizations on identifying, assessing, and mitigating cybersecurity risk in the supply chain at all levels of their organizations." To achieve that objective, the draft focuses on the integration of cybersecurity supply chain management into organizational risk management assessments. The notice promulgating the second version explains that it differs from the first insofar as the drafters "worked on making the guidance more consumable" and also added two additional appendices "focused on Federal departments and agencies." Notwithstanding the effort to make the document more consumable, it remains in many ways quite technical.

Notably, the draft includes Appendix C, which provides a risk exposure framework with numerous scenarios, including influence or control by foreign governments over suppliers, which is particularly relevant given the current concerns with hostile cyber actions by certain foreign governments, including Iran, Russia and China. Here too the comment period has now closed.

C. Software BOM

EO 14,028 directed the Department of Commerce, working with the National Telecommunications and Information Administration (NTIA), to develop the "minimum elements" of a Software Bill of Materials. On July 12, 2021, NTIA issued a report titled "The Minimum Elements For a Bill of Materials (SBOM)." The report defines an SBOM as "a formal record containing the details and supply chain relationships of various components used in building software." As reflected in the report, an SBOM is intended to facilitate the ability to identify software vulnerabilities and risks and a means to develop improved security tools and practices.

As called for by the EO, the NTIA report establishes the requested SBOM minimum elements and also "defines the scope of how to think about minimum elements, describes SBOM use cases for greater transparency in the software supply chain, and lays out options for future evolution." With respect to the minimum elements, the report lays out what it refers to as "three broad, interrelated areas:" Data Fields, Automation Support, and Practice and Processes.

NOTES

D. Zero Trust Architecture

The EO also requires agencies to develop their own plans for implementing "zero trust architecture." Zero Trust encompasses a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both *inside* and *outside* traditional network boundaries. Networks should be designed in a way to require "continuous verification" throughout the system. Zero Trust guards against internal threats, not only external ones, by denying an attacker that breaches a system the ability to roam freely (i.e., lateral movement) within the system.

In September, the government released several documents for public comment, seeking feedback on both OMB and CISA draft guidance documents to implement a Zero Trust cybersecurity policy government-wide.

1. OMB *Moving the U.S. Government Towards Zero Trust Cybersecurity Principles*, Draft for Public Comment (September 7, 2021)

The EO directs agencies to focus on meeting key baseline security measures including universal logging, multi-factor authentication (MFA), reliable asset inventories, ubiquitous use of encryption, and adopting a zero trust architecture. OMB's draft Federal Zero Trust Strategy states that "[t]o do this, the U.S. government's security architecture must avoid implicit trust in devices and networks, assume networks and other components will be compromised, and generally rely on the principle of least privilege." The Strategy says that "[w]hile the concepts behind zero trust architectures are not new, the implications of shifting away from 'trusted networks' are new to most enterprises, including many Federal agencies," and "this will be a journey for the Federal Government, and there will be learning and adjustments along the way as agencies and policies adapt to new practices and technologies."

The Strategy describes a federal Zero Trust architecture that:

- Bolsters identity practices.
- Relies on encryption and application testing instead of perimeter security.
- Recognizes every device and resource the government has.
- Supports intelligent automation of security actions.
- Enables safe and robust use of cloud services.

The Strategy requires government agencies to achieve specific Zero Trust security goals by the end of Fiscal Year (FY) 2024. Agencies have 60 days from the draft Strategy's publication to submit their implementation plan for these goals to OMB, along with a budget estimate, and 30 days to designate an agency "zero trust implementation lead" lead to coordinate the effort with OMB.

1. CISA *Moving the U.S. Government towards Zero Trust Cybersecurity Principles, Zero Trust Maturity Model* (September 7, 2021) and CISA *Cloud Security Technical Reference Architecture*

CISA's Zero Trust Maturity Model was developed to assist agencies as they implement the government-wide strategy (the Model was developed in June 2021 and shared with federal agencies for consideration and feedback before being publicly released in September 2021). The Model is intended to compliment OMB's Strategy and "to provide agencies with a roadmap and resources to achieve an optimal zero trust environment." The goals involve

achievements in identity management, device management, network security, application policy, and data protection.

CISA also separately released its Cloud Security Technical Reference Architecture (TRA) describing how the cloud can accelerate adoption of zero trust. The Cloud Security TRA was developed through a collaborative, multi-agency effort with contributions from the United States Digital Service (USDS), and the Federal Risk and Authorization Management Program (FedRAMP). The TRA provides agencies with guidance on the shared risk model for cloud service adoption, how to build a cloud environment, and how to monitor such an environment through robust cloud security posture management.

The OMB and CISA guidance materials were also informed by the following zero trust architecture developments across the government:

- NIST released a second draft of NIST SP 800-207 "Zero Trust Architecture" in February 2020.
- In July 2021, NIST's National Cybersecurity Center of Excellence (NCCoE) announced a new project with industry collaborators to develop zero trust architecture implementations for the government and the private sector. The project is limited to industry participants who sign cooperative research and development agreements (CRADAs) to work with the NCCoE. However, NIST has stated there will be opportunities for more direct engagement from academic institutions and government agencies through a new forum that goes beyond NCCoE's traditional community of interest model.
- DOD published its own DOD Zero Trust Reference Architecture in April, 2021. The development of the architecture was led by the Defense Information Systems Agency (DISA), in partnership with the DOD CIO's office, U.S. Cyber Command, and National Security Agency (NSA).

E. FAR Rulemakings

The EO directs the FAR Council to publish for public comment proposed contract language to address, among others: standardizing security incident reporting provisions government-wide; standardized common cybersecurity contractual requirements; and cybersecurity information-sharing with the federal government.

According to the EO, "current cybersecurity requirements for unclassified system contracts are largely implemented through agency-specific policies and regulations, including cloud-service cybersecurity requirements. Standardizing common cybersecurity contractual requirements across agencies will streamline and improve compliance for vendors and the Federal Government."

EO Section 2(i) directs the Department of Homeland Security (DHS) to "review agency-specific cybersecurity requirements that currently exist as a matter of law, policy, or contract and recommend to the FAR Council standardized contract language for appropriate cybersecurity requirements. Such recommendations shall include consideration of the scope of contractors and associated service providers to be covered by the proposed contract language."

The EO also directs OMB to evaluate current contract terms and restrictions of companies offering the federal government information technology (IT) and operational technology (OT) services to remove barriers to sharing "cyber threat and incident information" with agencies responsible "for inves-

tigating or remediating cyber incidents such as CISA, the Federal Bureau of Investigation (FBI) and the intelligence community.

In the Fall 2021 Unified Agenda of Regulatory and Deregulatory Actions, the FAR Council plans to release a notice of proposed rulemaking in February 2022 for two cases:

- FAR Case 2021-019, *Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems*, will standardize common cybersecurity contractual requirements across agencies for unclassified federal information systems, pursuant to DHS recommendations in accordance with sections 2(i) and 8(b) of the EO.
- FAR Case 2021-017, *Cyber Threat and Incident Reporting and Information Sharing*, will increase cyber threat and incident information sharing between the Government and certain providers, pursuant to OMB recommendations, in accordance with EO Sections 2(b)-(c), and DHS recommendations, in accordance with EO Section 8(b). In addition, the rule will require certain contractors to report cyber incidents to the Federal Government to facilitate effective cyber incident response and remediation, DHS recommendations in accordance with EO Section 2(g)(i).

II. UPDATED DOD CYBERSECURITY REQUIREMENTS – CMMC 2.0

On November 17, 2021, the DOD published an Advanced Notice of Proposed Rulemaking (ANPRM) previewing significant changes to its CMMC program. CMMC 2.0 was DOD's response to a months-long internal review spurred by more than 850 public comments in response to DOD's September 2020 "CMMC 1.0" interim rule. "CMMC 2.0" promises a more streamlined and flexible system for defense contractors and their suppliers to comply with CMMC and DOD's cybersecurity expectations, with practical changes coming into effect between 9 and 24 months after issuance.

CMMC 2.0 will replace the five-level model of CMMC 1.0 with three progressively more complex levels of cybersecurity requirements, each keyed to independently established standards (e.g., FAR and NIST requirements). The new model will also increase oversight of third-party assessors and eliminate all "maturity" requirements and CMMC-unique practices.

The new tiered requirements in the three-level model are as follows:

- Level 1 "Foundational" – Level 1 remains largely the same as in the prior model, with annual self-assessments and certifications by company leadership. Level 1 requires the same 15 controls, derived from FAR 52.204-21 "basic" controls required for protection of Federal Contract Information.
- Level 2 "Advanced" – Level 2 in CMMC 2.0 is based on the superseded CMMC 1.0 "Level 3," with a bifurcation of "prioritized acquisitions" and "non-prioritized acquisitions" in relation to the sensitivity of Controlled Unclassified Information (CUI) involved. As an example, prioritized acquisitions may involve CUI related to weapons systems, whereas nonprioritized acquisition might involve CUI related to military uniforms, though details on prioritization are expected in forthcoming rulemakings. Prioritized acquisitions will require an independent third-party assessment from a certified third-party assessing organization (C3PAO) every three years, while non-prioritized

acquisitions will require only an annual self-assessment. CMMC's new Level 2 reduces the number of required controls to the 110 controls included in NIST SP 800-171 Rev. 2, thereby eliminating what are now 20 additional Level 3 CMMC 1.0 controls.

- Level 3 "Expert" – CMMC's new Level 3 will replace existing Levels 4 and 5. Most notably, acquisitions at this level will require triennial government-led assessments (i.e., not by C3PAOs). Further, in addition to the 110 controls required for new Level 2, Level 3 certification will also require compliance with the controls in NIST SP 800-172.

The ANPRM states that the new CMMC 2.0 framework will be implemented by a pair of rules in both Title 32 (National Security) and Title 48 (FAR and DFARS).

In a notable departure from CMMC 1.0, the DOD will allow some acquisitions to satisfy requirements via plans of action and milestones (POAMs) (i.e., in lieu of actual compliance) under CMMC 2.0. Specifically, in limited circumstances, contractors with POAMs will be able to receive some contract awards while they make progress toward full compliance. DOD will not, however, accept a POAM for certain "high[ly] weighted" controls. Moreover, a company seeking to meet CMMC 2.0 requirements through a POAM must achieve a certain minimum threshold score. Further, eligible contractors must complete POAMs within 180 days of contract award after which a contracting officer may terminate the contract if controls have not yet been implemented. In addition to POAMs, CMMC 2.0 will also introduce the concept of waivers for certain mission-critical work. Such waivers will be strictly time-limited and may only be approved by senior DOD personnel.

On December 3, 2021, DOD released CMMC 2.0 "Scoping Guidance" for Levels 1 and 2. The Level 1 guidance focuses on identifying Federal Contract Information (FCI) Assets that process, store, or transmit FCI. Such assets are within the scope of the of the CMMC 2.0 self-assessment. The guidance also notes that so-called "specialized assets," such as government property and Internet of Things (IoT) devices are not within the scope of the self-assessment. The Level 2 scoping document describes four categories that are within the assessment scope: CUI, Security Protection Assets, Contractor Risk Managed Assets, and Specialized Assets. The scoping document also explains that "out-of-scope assets" are those that are unable to process, store, or transmit CUI because they are "physically or logically separated . . . from CUI assets."

On December 15, 2021, DOD released its Level 1 self-assessment guide and on December 20, 2021, the Level 2 Assessment Guide. The Level 1 Guide focuses on 17 practice requirements applied across five distinct areas: Access Control, Identification and Authorization, Media Protection, Physical Protection Systems and Communication Protection, and System and Information Integrity. The 17 practices are derived from SP 800-171 and SP 800-171A. The Level 2 Guide is additive to the Level 1 requirements and focuses on CUI; like the Level Guide 1, it focuses on SP 800-171 and SP 800-171A. As reflected in the ANPRM, the Level 2 Guide creates a two-tiered process under which contractors will need to undergo a triennial third-party assessment for programs that involve "critical national security information" and annual self-assessment for "select programs." Notably, the Guide further explains that contractors that self-assess will not be considered to hold a Level 2 certification.

NOTES

III. DOE CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

On July 21, 2021, the Department of Energy (DOE) released the next iteration of its Cybersecurity Capability Maturity Model (C2M2). DOE, *Cybersecurity Capability Maturity Model Version 2.0* (July 2021). Dubbed C2M2 Version 2.0, this release significantly builds upon Version 1.0, which was first rolled out in 2012 and underwent subsequent updates in 2014 and 2019. It also concludes DOE's 100-day Action Plan—a coordinated effort between DOE, the electricity industry, and CISA to safeguard critical U.S. electrical infrastructure against cyber threats.

Consistent with prior versions, C2M2 Version 2.0 encompasses 342 cybersecurity practices, which are grouped across ten domains (such as Risk Management; Situational Awareness; and Cybersecurity Architecture). The cybersecurity practices within a given domain are further organized by objective, and then ordered by maturity indicator level (MIL). C2M2 defines four MILs—0 through 3—to establish a "dual progression" of maturity. MILs are cumulative, meaning to attain a given maturity level, an organization must implement all practices indicated at that maturity level as well as at all lower maturity levels. The same is true at the domain level, whereby an organization must implement all domain objectives at a given maturity level to attain that maturity level.

Version 2.0 improves the C2M2 model by enhancing and streamlining cybersecurity practices to help energy sector organizations strengthen their operational resilience in order to confront modern day cyber threats and attacks against critical energy infrastructure. Specifically, Version 2.0 responds to emerging technologies, such as "cloud, mobile, and artificial intelligence," as well as to "evolving threats such as ransomware and supply chain risks." C2M2 Version 2.0 incorporates the following key approaches:

- Improved alignment with recognized industry best practices and cyber standards, such as the NIST Cybersecurity Framework and the updated NIST SP 800-53 "Security and Privacy Controls for Information Systems and Organizations."
- Establishes the new "Cybersecurity Architecture" domain to ensure energy sector organizations appropriately protect their networks and data. This domain encompasses the cybersecurity architecture and secure software development practices that were previously found in Version 1.0's "Cybersecurity Program Management" domain.
- Establishes the new "Third-Party Risk Management" domain, which replaces and revises the former "Supply Chain and External Dependencies Management" domain. This reorganization reflects entities' need to identify and oversee any third parties involved in the safeguarding of critical energy infrastructure.
- Revises the "Risk Management" domain to improve implementation and accessibility of guidance and relevant practices, such that entities can better identify, analyze, and respond to cyber threats.
- Integrates information sharing into the "Threat and Vulnerability Management" and "Situational Awareness" domains.
- Provides descriptive guidance to enable organizations to mature and refine their cybersecurity capabilities, regardless of organization size, structure, or industry.

DOE has been conducting industry piloting of C2M2 Version 2.0 since July 2021.

On November 24, 2021, the DOE published a notice seeking public comment on C2M2 Version 2.0 in order to inform future updates. 86 Fed. Reg. 67,038 (Nov. 24, 2021). Among other things, DOE sought industry input on: the usefulness of C2M2 practices to evaluate and improve an organization's cybersecurity capabilities; the comprehensiveness of Version 2.0's cybersecurity domains, objectives, and practices; the effectiveness of C2M2 guidance documentation; and other recommended improvements. Comments are due by February 10, 2022.

IV. DEVELOPMENTS IN THE NATIONAL CUI PROGRAM

As we've noted in previous papers, on September 14, 2016, the National Archives and Records Administration (NARA) released its CUI Final Rule, codified at 32 C.F.R. Part 2002, *Controlled Unclassified Information*, which formally identifies the approved categories and subcategories of federal CUI, establishes the official CUI Registry, and prescribes the use of NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" when CUI will reside on non-federal information systems. However, after five years, DOD is still the only agency explicitly mandating in its acquisition regulations that its covered contractors follow NIST SP 800-171 (as required in the NARA rule) for safeguarding CUI *on contractor systems*.

A. FAR Case 2017-016 Controlled Unclassified Information

This year, NARA announced in a November blog post that "one of the highest priorities of the CUI Executive Agent is getting a CUI FAR clause issued." The long anticipated FAR clause "will create a common mechanism to communicate which information contractors create for and receive from the Federal Government must be protected, how to protect it, and who it can be shared with…will be a standard vehicle for conveying whether CUI is involved in the contract and what the existing requirements are for safeguarding it [and] Contractors and Government officials will know the place in any solicitation or contract to find this information."

B. Updates to NIST 800-171 and NIST 800-172

NIST SP 800-171 established the 110 baseline security standards for government contractors that process, store, or transmit CUI. Revisions to this standard are tied to those associated with NIST SP 800-53. As we noted in last year's paper, NIST published Revision 5 to NIST SP 800-53 in September 2020, which was described by NIST as a "complete renovation" and the "first comprehensive catalog of security and privacy controls that can be used to manage risk for organizations of any sector and size, and all types of systems--from super computers to industrial control systems to Internet of Things (IoT) devices." NIST SP 800-53 Rev. 5. was published seven months *after* the last update to SP 800-171 (Revision 2). As a result, NIST is in the process of determining what changes need to made to 800-171 to align with the updated controls in 800-53, and anticipates publishing 800-171 Revision 3 in 2022.

Separately, as part of its overhaul of CMMC (discussed above), DOD has said it has plans to propose additional controls from its old CMMC model for inclusion in the next update to NIST SP 800-171. As part of the CMMC 2.0 reorganization, the DOD consolidated the number of maturity levels from five to three and removed the 20 controls that go beyond SP 800-171 from the new

level two. However, DOD has stated that some of those requirements will be proposed to NIST for inclusion in the next revision of NIST SP 800-171 with the end result that they will become part of the technical standards baseline itself (i.e., listed in NIST SP 800-171) rather than layered on by the CMMC program.

In July 6, 2020, NIST published draft SP 800-172, a companion publication to SP 800-171 that includes additional protections for CUI from advanced persistent threats (APTs). The final version of SP 800-172 was released in February 2021. While SP 800-171 is focused on *confidentiality,* the enhanced controls in SP 800-172 address protecting the *confidentiality, integrity,* and *availability* of CUI on contractor information systems from APT. Agencies are expected to identify and selectively apply enhanced security SP 800-172 protections in addition to the basic and derived requirements in SP 800-171. A decision to select a particular set of enhanced security requirements from SP 800-172 should be based on the specific mission and business protection needs of the agency, and informed by ongoing risk assessments.

In April 2021, NIST published draft SP 800-172A, "Assessing Enhanced Security Requirements for Controlled Unclassified Information" which will provide federal agencies and nonfederal organizations with assessment procedures that can be used to carry out assessments of the enhanced requirements in SP 800-172. NIST has stated it plans to publish the final version of SP 800-172A in the first quarter of 2022.

V. U.S. CYBERSPACE SOLARIUM COMMISSION

As we noted in last year's article, the National Defense Authorization Act (NDAA) for FY 2021 (H.R. 6395) reauthorized the U.S. Cyberspace Solarium Commission through December 2021. The Commission was charged with monitoring federal implementation of prior cybersecurity policy recommendations, as well as revising, amending, or making additional recommendations to advance the nation's strategic approach to cybersecurity.

On August 12, 2021, the Commission published its 2021 Annual Report on Implementation. The Report tracks the government's adoption and implementation of the Commission's policy recommendations proposed in its March 2020 "Final Report" and subsequent white papers. The Commission touts that approximately 35% of its 82 recommendations have been implemented or are nearing full implementation, while 44% are on track for full implementation. The Report highlights the following key achievements:

- ***Stand-up of the Office of the National Cyber Director (ONCD) in the White House.*** Congress established the ONCD this year and confirmed Chris Inglis as the nation's first National Cyber Director (NCD). The NCD advises the President on critical cybersecurity policy and strategy, while guiding the nation's global engagement with cybersecurity stakeholders. Funding is expected in FY 2022 to build out the ONCD's operations.
- ***Strengthening the Authorities of the U.S. Cybersecurity and Infrastructure Agency (CISA).*** The Commission recommended several measures, such as granting subpoena power and engaging in threat hunting on federal networks, to strengthen CISA's authorities and to achieve better outcomes from private sector collaboration. Several of these recommendations were included in the FY 2021 NDAA. Moreover, the American Rescue Plan Act of 2021 included $650 million to support vital CISA cybersecurity operations.

- ***Progress towards developing a National Cyber Strategy.*** One of the Commission's major recommendations was the development of a national cyber strategy. The Report points to President Biden's May 12, 2021 "Executive Order on Improving the Nation's Cybersecurity" as a significant sign the administration is prioritizing development of this much-needed strategy.
- ***Establishment of a Cyber Response and Recovery Fund.*** The Commission recommended the creation of a Cyber Response and Recovery Fund to support agencies' cyber capabilities when responding to a significant cyber incident. President Biden's 2021 Budget Request included $20 million for the establishment of this fund, and the Senate introduced the Cyber Response and Recovery Act of 2021 (S. 1316) to codify the process of declaring a significant cyber event.

Despite these significant achievements to improve the nation's cybersecurity, the Report highlights the increasing frequency and sophistication of cyber threats (such as the SolarWinds supply chain attack and the Colonial Pipeline ransomware attack) as a reminder of the work that remains to secure the nation's critical infrastructure. For example, several key initiatives remain in limbo pending much-needed appropriations and ongoing congressional negotiations of core legislative details. Critical recommendations facing significant barriers to implementation include establishing dedicated congressional committees on cybersecurity, enacting a national data security and privacy protection law, developing public-private partnerships to share threat intelligence, and establishing a federal cyber statistics bureau to create much-needed incident response data for use in policy decision-making.

The Commission officially sunset on December 21, 2021, although the involved lawmakers have publicly affirmed their intention to continue pursuing these initiatives as part of a new "Solarium 2.0" nonprofit organization.

VI. DOJ CYBER-FCA INITIATIVES

On October 6, 2021, DOJ announced its Civil Cyber-Fraud Initiative that will use the False Claims Act (FCA) against government contractors and grant recipients allegedly lacking robust cybersecurity protections. In relation to the FCA, the Initiative will hold companies accountable for the following:

- Knowingly providing deficient cybersecurity products or services
- Knowingly misrepresenting cybersecurity practices
- Knowingly violating obligations to monitor and report cybersecurity incidents and breaches

The first stated benefit of the initiative is "building broad resiliency against cybersecurity intrusions across the government, the public sector and key industry partners." Other benefits listed similarly emphasize the importance of promoting strong cybersecurity policies by government contractors, with potential FCA cases providing motivation.

1 Mike Vernick would like to acknowledge the contributions to this paper made by numerous Akin Gump colleagues, including his partners Natasha Kohne and Michelle Reed, and associate Chris Chamberlain.

2 Mike Scheimer would like to acknowledge the contributions to this paper made by associate Lauren Olmsted.