June 2021 Developments Under the Executive Order on Improving the Nation's Cybersecurity

By Susan B. Cassidy, Robert Huffman & Ryan Burnette on July 1, 2021
Posted in Cybersecurity, Information Technology Contracting, Supply Chain

On May 12, 2021 the Biden Administration issued an "Executive Order on Improving the Nation's Cybersecurity" (EO). Among other things, the EO sets out a list of deliverables from a variety of government entities. A number of these deliverables were due in June, including a definition of "critical software," the minimum requirements for a software bill of materials, and certain internal actions imposed on various federal agencies.

Developments Affecting Enhancement of Software Supply Chain Security

Definition of Critical Software. Section 4 of the EO stated that the "development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors." The EO cites a "pressing need" for mechanisms to ensure the "security and integrity" of "critical software." The EO broadly defines critical software as "software that performs functions critical to trust" and tasks the Secretary of Commerce, through the National Institute of Standards and Technology (NIST) to develop a definition of critical software that could be used in forthcoming regulations and guidance – including guidance required by the EO on identifying practices that enhance the security of the software supply chain.

On June 25, 2021, NIST issued a white paper providing a definition of critical software. The white paper followed a workshop that NIST held on June 2-3, 2021 with over 1400 participants and 150 position papers submitted for NIST's consideration. In addition to private industry, NIST solicited input from the public as well as reportedly from several government agencies – including the Cybersecurity and Infrastructure Security Agency, the Office of Management and Budget (OMB), the Office of the Director of National Intelligence (ODNI) and the National Security Agency – to help define what critical software means.

NIST's definition is broad and defines critical software as

any software that has or has direct software dependencies upon, one or more components with at least one of these attributes:

- *Software that is designed to run with elevated privilege or manage privileges;*
- *Software that has direct or privileged access to networking or computing resources;*

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

According to NIST, this definition preliminarily includes operating systems, web browsers, hypervisors, endpoint security tools, identity and access management applications, network monitoring tools, backup, recovery, and remote storage tools, and other categories of software.

In explaining the definition, NIST expressed its view that the EO's implementation "must take into consideration how the software industry functions, including product development, procurement, and deployment." Further, NIST explained that the term "critical" as used in the EO is not based not on the context of use, "but instead focuses on critical functions that address underlying infrastructure for cyber operations and security." Some limited use cases – such as software solely used for research or testing that is not deployed in production systems – are outside of the scope of this definition.

Finally, although the definition applies to all forms of software, NIST recommends that the initial EO implementation phase focus on standalone, on-premises software that has security-critical functions or poses similar significant potential for harm if compromised. NIST indicated that later implementation of the EO could expand to other forms of software such as software that controls access to data, cloud-based and firmware to name a few.

Other Developments

Software Bill of Materials Minimum Requirements. Section 4(f) of the EO requires the National Telecommunications and Information Administration (NTIA) to publish the minimum elements of a Software Bill of Materials (SBOM), which the EO defines as "a formal record containing the details and supply chain relationships of various components used in building [the] software." In preparing to meet the July 11, 2021 deadline for publishing the minimum elements for SBOMs, NTIA issued a request for public comment on the minimum elements for SBOMs and the factors that should be considered in requesting, producing, distributing, and consuming such items.

NTIA's request notes that an SBOM is similar to a "list of ingredients" and thereby promotes transparency in the software supply chain. NTIA proposed a definition of the minimum elements of an SBOM that encompasses three broad, inter-related features: (1) required data fields; (2) operational considerations; and (3) support for automation. Data fields suggested include "supplier name," "component name," and "cryptograph hash of the component," among others. Operational considerations include a set of operational and business decisions and actions that establish the practice of requesting, generating, sharing, and consuming SBOMs, including "frequency," "depth," and "delivery." Automation support relates to whether the SBOM can be automatically generated and is machine-readable, which is "[a] key element for SBOM to scale across the software ecosystem."

July 2021 Developments Under the Executive Order on Improving the Nation's Cybersecurity

By Robert Huffman, Susan B. Cassidy & Ryan Burnette on July 27, 2021

Posted in Commercial Items, Cybersecurity, Information Technology Contracting, Supply Chain

On May 12, 2021, the Biden Administration issued an Executive Order on Improving the Nation's Cybersecurity (the "EO"). The EO sets out a list of deliverables due from a number of governmental entities in June 2021 and successive months. Our overall summary of the EO and its deliverables can be found here, and our discussion of the EO deliverables that were due in June 2021 can be found here. This blog addresses the EO deliverables in July 2021.

Developments Affecting Enhancement of Software Supply Chain Security

NIST Publishes Guidance on Security Measures for Critical Software Use

On June 25, 2021, the National Institute of Standards and Technology ("NIST") published a white paper containing a definition of "critical software" for purposes of Section 4 of the EO, "Enhancement of Software Supply Chain Security." Section 4(i) of the EO requires NIST, in consultation with the Cybersecurity & Infrastructure Security Agency ("CISA") and the Office of Management and Budget ("OMB"), to publish guidance by July 11 outlining security measures for critical software as defined by NIST, "including applying practices of least privilege, network segmentation, and proper configuration." On July 9, 2021, NIST published the guidance called for by Section 4(i).

NIST's guidance is aimed at federal agency use of "EO-critical software" – i.e., software defined by NIST as critical software under Section 4(g) of the EO by federal agencies in their operational environments.[1] Although the EO was not explicit as to whether the guidance would extend beyond the government and its contractors, the guidance that was issued does not purport to cover development or acquisition of EO-critical software, nor does it purport to cover use of EO-critical software by non-governmental organizations.

The substance of the guidance consists of two main components: (a) Security Measure objectives, and (b) the Security Measures themselves. The guidance explicitly makes these objectives and security measures applicable to both EO-critical software ***and*** to EO-critical ***software platforms***, which it defines as the platforms on which EO-critical software runs, including endpoints, servers, and cloud resources. Thus, it would be a mistake to view the objectives and security measures set forth in the guidance as limited to software only. The guidance defines the Objectives as:

1. *Protect EO-critical software and EO-critical software platforms (the platforms on which EO-critical software runs, such as endpoints, servers, and cloud resources) from unauthorized access and usage.*
2. *Protect the confidentiality, integrity, and availability of data used by EO-critical software and EO-critical software platforms.*
3. *Identify and maintain EO-critical software platforms and the software deployed to those platforms to protect the EO-critical software from exploitation.*
4. *Quickly detect, respond to, and recover from threats and incidents involving EO-critical software and EO-critical software platforms.*
5. *Strengthen the understanding and performance of humans' actions that foster the security of EO-critical software and EO-critical software platforms.*

Each of these objectives has several security measures associated with it. For example, to protect EO-critical software and EO-critical software platforms from unauthorized access and usage under Objective 1, one of the security measures is to "[u]se multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms." The FAQs indicate that "an example of a verifier impersonation-resistant protocol is client-authenticated Transport Layer Security (TLS)." Implementation of these security measures could represent a significant effort for agencies, depending on the nature and scale of the systems that they operate.

The security measures are largely sourced from other publications, including NIST SP 800-53 and NIST's cybersecurity framework. Although the measures are intended to apply to agencies, NIST indicated in the response to a separate FAQ that "[t]he security measures for using EO-critical software could be applied to cloud-based environments by cloud service providers."

NIST Publishes Guidelines Recommending Minimum Standards for Vendor Verification of Their Software Source Codes

EO Section (4r) requires NIST to publish guidelines recommending minimum standards for vendors' testing of their software source code, including identifying recommended types of manual or automated testing (such as code review tools, static and dynamic analysis, software composition tools, and penetration testing) by July 11, 2021. On July 9, NIST published these guidelines. NIST indicated that "[w]hile the EO uses the term 'vendors' testing,' the intent is much broader and includes developers as well." Given the broad scope of the potential application of the guidance and its application to vendors and software developers, it is possible that federal contractors could see these requirements imposed by certain agencies as part of their contracts with those agencies.

NIST's recommended minimum verification standards consist of Technique Classes, Techniques, and Descriptions and References to Recommended Minimums Documents. The Technique Classes are: (1) Threat Modeling; (2) Automated Testing; (3) Code-Based (Static) Analysis; (4) Dynamic Analysis; (5) Check Included Software; and (6) Fix Bugs. Each of these Technique Classes includes one or more specific techniques. For example, the Code-Based (Static) Analysis technique class includes the "Use a code scanner to look for top bugs"

technique and the "Review for hardcoded secrets" technique. The guidelines provide descriptions and references for these and all other techniques specified.

The FAQs included in the guidelines explain why the guidelines refer to source code "verification" rather than "testing," which is the term used in the EO. The response to FAQ #4 asserts that the term "testing" is often used to describe dynamic analysis only, and that the term "verification" is more technically accurate given "the myriad types of software testing referred to in the EO." It further states that use of the term verification "ensures that the goal of the EO is met." FAQ #3 explains why NIST extended the minimum standards to both vendor and developer verification even though the EO refers only to vendors. The response to FAQ #3 notes that the software vendor and developer are not always the same, and that "verification should be done as early in the software development life cycle (SDLC) as possible, which will be by the developer," while a vendor who is not also the software's developer "should also perform verification but will not have the opportunity to be involved early in the process."

Finally, FAQ #1 makes clear that the source code minimum verification standards "are guidelines and remain voluntary." However, section (4e) of the EO requires NIST to develop guidance for "employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at minimum prior to product, version, or update release…." FAQ #1 states that NIST anticipates that the guidance it develops under section (4e) will reference the software source code verification guidelines.

Recommendations Regarding FAR and DFARS Contract Language

Recommendations Regarding Agency-Specific Cybersecurity Requirements

Section 2(i) of the EO directs CISA, in consultation with the National Security Agency ("NSA"), the OMB Director, and the General Services Administration ("GSA") Administrator, to review agency-specific cybersecurity requirements that currently exist as a matter of law, policy, or contract, and to recommend to the Federal Acquisition Regulation ("FAR") Council by July 11, 2021 "standardized contract language for appropriate cybersecurity requirements." The section states that CISA's recommendations "shall include consideration of the scope of contractors and associated service providers to be covered by the proposed contract language." This language is likely to be of great interest to the federal contractor community, as any recommended requirements could become a condition for certain contract awards.

It is unclear at this time whether CISA submitted any recommended standardized contract language for cybersecurity requirements to the FAR Council pursuant to section 2(i). CISA's website notes that pursuant to the EO, it "will work with OMB to recommend contract language that makes sharing critical data easier…." Even if CISA has recommended language, we understand that it is CISA's policy not to publicly disclose its recommended language until the FAR Council proposes standardized contract language for public notice and comment, which it is

required by EO section 2(j) to do within 60 days of receiving recommended language from CISA.

Recommendations Regarding FAR and DFARS Contract Requirements and Language for IT and OT Service Providers

Section 2(b) of the EO requires OMB, in consultation with the Secretary of Defense, the Attorney General, the secretary of Homeland Security, and the Office of the Director of National Intelligence, to review the FAR and Defense Federal Acquisition Regulation Supplement ("DFARS") contract requirements and language for contracting with information technology ("IT") and operational technology ("OT") service providers and to recommend updates to such requirements and language to the FAR Council and other appropriate agencies by July 11, 2021. The section further requires that the recommended contract language shall include descriptions of contractors to be covered by the language, and shall be designed to ensure, among other things, that such service providers collect, report, and preserve data relevant to cyber incidents or potential cyber incidents on all information systems over which they have control, including systems operated on behalf of agencies.

It is unclear at this time whether OMB has completed its review of the relevant FAR and DFARS provisions or submitted any recommended contract language to the FAR Council for IT and OT service providers pursuant to section 2(b) of the EO.

Federal Network Infrastructure Modernization, Including Cloud Services

Section 3(b) of the EO requires the head of each federal agency, by July 11, 2021, to (a) update existing agency plans to prioritize resources for the adoption and use of cloud technology as outlined in relevant OMB guidance, (b) develop a plan to implement Zero Trust Architecture, including migration steps that NIST has outlined in guidance and standards, and (c) provide a report to OMB discussing the agency's cloud technology and Zero Trust Architecture plans. Section 3(c)(iii) of the EO requires CISA, also by July 11, to develop and issue a cloud service governance framework for federal civilian agencies. It is unclear at this time whether either of these deadlines were met.

National Security Systems Requirements

Section 9(a) of the EO requires the NSA, in coordination with the Director of National Intelligence and the Committee on National Security Systems, to adopt requirements for National Security Systems ("NSSs") by July 11, 2021, that are equivalent to or exceed the cybersecurity requirements set forth in the EO that are not otherwise applicable to NSSs. In general, an NSS is an unclassified information system that involves intelligence activities, cryptologic activities related to national security; command and control of military forces; equipment that is an integral part of a weapon or weapons system; or is critical to the direct

fulfillment of military or intelligence missions. Under the EO, any such requirements shall be codified in a National Security Memorandum ("NSM"), but until such time as that NSM is issued, no programs, standards, or requirements established pursuant to the EO shall apply with respect to NSSs.

[1] As discussed in our prior post, NIST defined EO-Critical Software 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.

August 2021 Developments Under President Biden's Cybersecurity Executive Order

By Robert Huffman, Susan B. Cassidy & Ryan Burnette on September 7, 2021
Posted in Cybersecurity, Defense Industry, Information Technology Contracting

This blog continues Covington's review of important deadlines and milestones in implementing the Executive Order on Improving the Nations' Cybersecurity (E.O. 14028, or the "Cyber EO") issued by President Biden on May 12, 2021. Previous blogs have discussed developments under the Cyber EO in June 2021 and July 2021. This blog focuses on developments affecting the EO that occurred during August 2021.

The Cyber EO requires federal agencies to meet several important deadlines in August 2021. These deadlines are in the areas of enhancing critical software supply chain security, improving the federal government's investigative and remediation capabilities, and modernizing federal agency approaches to cybersecurity. In addition, the National Institute of Standards and Technology ("NIST") took several significant actions related to supply chain security in August 2021, not all of which were driven by deadlines in the Cyber EO. This blog examines the actions taken by federal agencies to meet the EO's August deadlines as well as the NIST actions referred to above.

A. Enhancing Critical Software Supply Chain Security

1. *Actions Taken By OMB During August 2021*

Section 4(a) of the Cyber EO states that the security and integrity of "critical software" is of particular concern, and that the federal government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software. Pursuant to section 4(g) of the EO, NIST published a definition of the term "critical software" on June 25, 2021. Subsequently, on July 8, 2021, NIST published guidance to federal agencies on security measures for critical software. These developments are discussed in greater detail in our blogs on the June and July 2021 Cyber EO developments.

Section 4(j) of the EO requires the Office of Management and Budget ("OMB") to take appropriate steps by August 10, 2021 to require that agencies comply with the July 8 critical software security guidance issued by NIST. On August 10, 2021, Shalanda Young, the Acting Director of OMB, issued a Memorandum to the Heads of Executive Departments and Agencies entitled "Protecting Critical Software Through Enhanced Security Measures" (the "August 10 Memo").

The August 10 Memo sets out a "phased approach" for agency implementation of the NIST guidance. During the initial phase, agencies are required to focus on identifying and securing stand-alone, on-premise software that performs "security-critical functions or poses similar

significant potential for harm if compromised." Such software includes applications that provide the following categories of service:

- 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
- backup/recovery and remote storage

Along these lines, during the initial phase the August 10 Memo requires each agency to identify by October 10, 2021 all "critical software" as defined by NIST that falls within the categories of service described above that is in use or in the process of acquisition by the agency. The August 10 Memo further provides that each agency must implement the security measures designated in NIST's July 8 guidance for all categories of critical software included in the initial phase by August 10, 2022.

The August 10 Memo states that OMB will address subsequent phases of implementation in the future for additional categories of software as determined by CISA. The Memo states that the following categories of software, among others, will be addressed in these future phases:

- software that controls access to data;
- cloud-based and hybrid software;
- software development tools, such as code repository systems, testing software, integration software, packaging software, and deployment software;
- software components in boot-level firmware; and
- software components in operational technology.

2. Actions Taken by NIST During August 2021

The Biden Administration announced at a "Cybersecurity Summit" held at the White House on August 25, 2021 that NIST would collaborate with industry and other partners to develop a new framework for improving the security and integrity of the technology supply chain. The Administration states that this framework will serve as guidance to public and private entities on how to build secure technology and how to assess the security of technology, including open-source software, in their supply chains. This new framework will focus on promoting the development and adoption of international standards.

In a related development, a NIST spokesman announced on August 25, 2021 that NIST will delay issuance of a second draft (update) of SP 800-161 Rev. 1, "Supply Chain Risk Management", from September 2021 until October or November 2021 in order to incorporate

requirements imposed by the Cyber EO. In particular, Section 4(c) of the EO requires NIST to publish by November 8, 2021 preliminary guidelines for enhancing software supply chain security based on input from federal agencies, private industry, and academia that NIST received in June and July 2021. The NIST spokesperson stated that delaying the issuance of the NIST SP 800-161 Rev. 1 update would allow the agency to meet the EO's November 8 deadline for preliminary guidance on enhancing software supply chain security. It is unclear whether the update to SP 800-161 is the same as the new NIST framework for improving the security and integrity of the technology supply chain that the Biden Administration announced at the White House Cybersecurity Summit.

On August 24, 2021, NIST released the final version of NISTIR 8259B, "IOT Non-Technical Supporting Capability Core Baseline". This document complements NISTIR 8259A, "Core Device Cybersecurity Capability Baseline (May 2020), which is NIST's guide to the technical aspects of manufacturing secure Internet of Things ("IOT") devices and products. The document describes four recommended non-technical supporting capabilities related to the lifecycle of cybersecurity management that manufacturers should implement, including (1) documentation, (2) information and query reception, (3) information dissemination, and (4) education and awareness. Together, NISTIR 8259A and NISTIR 8259B are intended to define a baseline set of activities that manufacturers should undertake during the planning, development, and operational life of IOT devices to address the cybersecurity needs and goals of their customers.

On August 31, NIST issued a draft White Paper setting forth criteria that can be used to create the pilot labelling program for consumer IOT devices contemplated by Section 4 of the Cyber EO. This program is intended to educate the public on the security capabilities and vulnerabilities of IOT devices and software development practices. The White Paper notes among other things that in line with the direction set forth by the Cyber EO, IoT products must reflect increasingly comprehensive levels of testing and assessment, and that "[m]ore cybersecurity controls may be needed for devices that pose inherently greater risks such as a door lock or stove." The White Paper notes that a label should clearly convey information to consumers about elevated security capabilities, and that it should be understandable and actionable by the consumer. The White Paper states that NIST plans to hold a workshop on September 14 and 15, 2021, to obtain comments and other input on the pilot labelling program.

B. Improving the Federal Government's Cyber Investigative and Remediation Capabilities

Section 8(c) of the Cyber EO requires OMB, in consultation with the Secretaries of Commerce and DHS, to formulate policies for agencies to establish requirements for logging, log retention, and log management that ensure centralized access and visibility for the highest level security operations center ("SOC") of each agency. On August 27, 2021, the OMB Director issued a Memorandum to the heads of federal agencies regarding the logging, log retention, and log management requirements of EO section 8(c) (the "August 27 Memo"). The August 27 Memo also establishes requirements for agencies to increase the sharing of such information, as needed and appropriate, to accelerate incident response efforts and to enable more effective defense of federal information and agencies.

Section 1 of the August 27 Memo establishes an "Event Logging ("EL") maturity model that includes the four "Logging Tiers" described in the following table:

Event Logging Tiers	Rating	Description
EL0	Not Effective	Logging requirements of highest criticality are either not met or are only partially met
EL1	Basic	Only logging requirements of highest criticality are met
EL2	Intermediate	Logging requirements of highest and intermediate criticality are met
EL3	Advanced	Logging requirements at all criticality levels are met

The August 27 Memo requires each federal agency to assess its current logging maturity against the four tiers in the Memo's maturity model and identify any resource and implementation gaps that may exist relative to the respective requirements of each of those tiers. Agencies are required to report their assessments and gap analyses to OMB by October 27, 2021. In addition, the August 27 Memo requires each agency to reach the EL Tier 1 Maturity level by August 27, 2022, the EL Tier 2 Maturity level by February 27, 2023, and the EL Tier 3 Maturity level by August 27, 2023.

C. Modernizing Federal Agency Approaches To Cybersecurity

Section 3(c) of the Cyber EO states that federal agencies should migrate to cloud technology in a coordinated, deliberate way that adopts Zero Trust Architecture as practicable. The EO directs CISA to modernize its current cybersecurity programs, services, and capabilities to be fully functional with cloud-computing environments that have Zero Trust Architecture. The EO also directs CISA, in consultation with the GSA's FedRAMP Program, to develop security principles governing Cloud Service Providers ("CSPs") for incorporation into agency modernization efforts.

To implement these requirements, Section 3(c) imposes an August 10, 2021 deadline for completion of the following:

- OMB's development of a Federal cloud-security strategy and its issuance of guidance to agencies that seeks to ensure that they fully understand and effectively address the risks of using cloud-based services and to move them closer to Zero Trust Architecture.
- CISA's issuance of cloud-security technical reference architecture documentation for civilian agencies that illustrates recommended approaches to cloud migration and data protection for agency data collection and reporting.
- Evaluation by each federal agency of the types and sensitivity of its unclassified data that includes appropriate processing and storage solutions for such data, with priority on identifying that data that is most sensitive and under the greatest threat.

It is unclear what, if any, actions were taken by OMB, CISA, or federal agencies to implement these requirements during August 2021.

September 2021 Developments Under President Biden's Cybersecurity Executive Order

By Robert Huffman, Susan B. Cassidy, Ryan Burnette & Nooree Lee on October 1, 2021
Posted in Cybersecurity, Government Contracts Regulatory Compliance, Information Technology Contracting

This is the fifth in a series of Covington blogs on implementation of Executive Order 14028, "Improving the Nation's Cybersecurity", issued by President Biden on May 12, 2021 (the "Cyber EO"). The first blog summarized the Cyber EO's key provisions and timelines, and the second, third, and fourth blogs described the actions taken by various federal government agencies to implement the EO during June, July, and August 2021, respectively. This blog summarizes key actions taken to implement the Cyber EO during September 2021.

I. Actions Taken During September 2021 to Modernize Federal Government Cybersecurity

The Office of Management and Budget (OMB) publically released a draft zero trust architecture strategy for federal agencies on September 9, 2021. On that same day, the Cybersecurity and Infrastructure Agency (CISA) issued two draft documents designed to further OMB's zero trust strategy: the Zero Trust Maturity Model and the Cloud Security Technical Reference Architecture. Each of these documents was required by Section 3 of the Cyber EO to modernize and standardize federal government agency approaches to cybersecurity.

The OMB draft zero trust strategy states that the Federal Government can no longer depend on perimeter-based defenses to protect critical systems and data in the current threat environment, and that meeting these threats "will require a major paradigm shift in how Federal agencies approach cybersecurity" — namely, migration to a Zero Trust Architecture. The draft strategy identifies the "foundational tenet" of Zero Trust as "no actor, system, network, or service operating outside or within the perimeter can be trusted. Instead, we must verify anything and everything attempting to establish access." The draft states that the purpose of the strategy as "to put all Federal agencies on a common roadmap [to zero trust] by laying out the initial steps agencies must take to enable their journey toward a highly mature zero trust architecture."

The draft strategy would require agencies to achieve certain specified zero trust security goals by the end of FY2024. These goals are grouped according to five "pillars" underlying the foundation of zero trust. These pillars are:

- Identity: Agency staff use an enterprise-wide identity to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks.

- Devices: The Federal Government has a complete inventory of every device it operates and authorizes for Government use, and can detect and respond to incidents on those devices.
- Networks: Agencies encrypt all DNS requests and HTTP traffic within their environment, and begin segmenting networks around their applications. The Federal government identifies a workable path to encrypting emails in transit.
- Applications: Agencies treat all applications as internet-connected, routinely subject their applications to rigorous testing, and welcome external vulnerability reports.
- Data: Agencies are on a clear, shared path to deploy protections that make use of thorough data categorization. Agencies take advantage of cloud security services to monitor access to their sensitive data, and have implemented enterprise-wide logging and information sharing.

The draft strategy provides considerable detail regarding the goals associated with each of the pillars described above. In addition, the draft strategy requires each agency to update its zero trust architecture implementation plan to incorporate these requirements and to submit its updated plan to OMB within 60 days after the draft strategy becomes final.

The draft CISA Zero Trust Maturity Model issued on September 9 identifies three stages of implementation for each of the five foundational "pillars" identified in the draft OMB strategy: "Traditional"; "Advanced"; and "Optimal". The model describes each of these stages as follows:

- Traditional: Manual configurations and assignment of attributes, static security policies, pillar-level solutions with coarse dependencies on external systems, least-function established at provisioning, proprietary and inflexible pillars of policy enforcement, manual incident response and mitigation deployment.
- Advanced: Some cross-pillar coordination, centralized visibility, centralized identity control, policy enforcement based on cross-pillar inputs and outputs, some incident response to pre-defined mitigations, increased detail in dependencies with external systems, some least-privilege changes based on posture assessments.
- Optimal: Fully automated assigning of attributes to assets and resources, dynamic policies based on automated/observed triggers, assets have self-enumerated dependencies for dynamic least-privilege access (within thresholds), alignment with open standards for cross-pillar operability, centralized visibility with historian functionality for point-in-time recollection of state.

CISA's draft maturity model provides considerable additional detail regarding each of the above maturity stages. It also identifies current and expected services and offerings by CISA that can help an agency reach a higher stage of zero trust maturity.

Finally, CISA's Cloud Security Technical Reference Architecture provides guidance to federal agencies regarding the advantages and risks of adopting cloud-based services as they move toward zero trust architecture. The Cloud Security Technical Reference Architecture recommends approaches to cloud migration and data protection for agency data collection and reporting that leverages Cloud Security Posture Management (CSPM). The Architecture document defines CSPM as a continuous process of monitoring a cloud

environment; identifying, disclosing, and mitigating cloud vulnerabilities; and improving cloud security.

II. Actions Taken During September 2021 to Enhance Software Supply Chain Security

The National Institute of Standards and Technology (NIST) held a public workshop on September 14 and 15, 2021, to obtain feedback from government agencies, industry, and other sectors on its draft criteria for pilot labelling programs for (1) consumer software and (2) consumer Internet of Things (IoT) devices required by section 4 of the Cyber EO. Among the issues discussed at the workshop were whether labelling should be voluntary or mandatory and what methods should be used for conformity assessment and attestation with respect to consumer software and IoT device labels. A NIST spokesperson stated at the meeting that NIST does not intend to establish its own labelling programs, but rather is focused on developing a baseline for the contents of consumer software and IoT labels. NIST has also stated that it plans to issue a second draft of labelling baseline criteria in October 2021 based on input from the September 14-15 workshop, and to meet the February 2022 deadline in the Cyber EO for publication of the final baseline.

October 2021 Developments Under President Biden's Cybersecurity Executive Order

By Robert Huffman, Susan B. Cassidy, Ashden Fein & Ryan Burnette on November 4, 2021
Posted in Cybersecurity, Government Contracts Regulatory Compliance, Information Technology Contracting

This is the sixth in the series of Covington blogs on implementation of Executive Order 14028, "Improving the Nation's Cybersecurity," issued by President Biden on May 12, 2021 (the "Cyber EO"). The first blog summarized the Cyber EO's key provisions and timelines, and the second, third, fourth, and fifth blogs described the actions taken by various federal agencies to implement the EO during June, July, August, and September 2021, respectively. This blog summarizes key actions taken to implement the Cyber EO during October 2021.

Although the recent developments this month are directly applicable to the U.S. Government, the standards being established for U.S. Government agencies could be adopted as industry standards for all organizations that develop or acquire software similar to various industries adopting the NIST Cybersecurity Framework as a security controls baseline.

NIST Publishes Preliminary Guidelines for Enhancing Software Supply Chain Security

Section 4(c) of the Cyber EO directs NIST to publish preliminary guidelines for enhancing software supply chain security by November 8, 2021. NIST issued these preliminary guidelines on October 28, 2021 as part of a second draft of NIST Special Publication 800-161 Revision 1, "Supply Chain Risk Management Practices for Systems and Organizations." The preliminary guidelines, which are specifically addressed in Appendix F to Draft Revision 1, but are also incorporated throughout the document, describe key cybersecurity supply chain risk management (C-SCRM) practices for managing exposures to cybersecurity risks, threats, and vulnerabilities throughout the supply chain and developing appropriate response strategies presented by the supplier, the supplied products, services, and the supply chain. The guidelines also provide a general prioritization of such practices (i.e., Foundational, Sustaining, and Enabling) for enterprises to consider as they implement C-SCRM.

In preparing the updated draft following the release of the Cyber EO, NIST translated the Cyber EO's Section 4 software supply chain directives into three targeted initiatives:

- Critical Software Definition and Security Measures;
- Recommended Minimum Standard for Vendor or Developer Verification of Code; and
- Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software.

NIST will accept comments on the preliminary guidelines through December 5, 2021. The Cyber EO requires NIST to publish final guidelines for ensuring software supply chain security by February 2022. While these guidelines will initially be applicable only to federal agencies, the head of cyber response and policy at the National Security Council, Jeff Greene, stated recently that a goal of the Cyber EO was "spillover" of NIST's software security guidelines to private entities, presumably (in the case of government contractors and subcontractors) through the use of standardized FAR clauses contemplated elsewhere in the Cyber EO.

NIST Announces Virtual Workshop on November 8 to Discuss Artifacts Used in Developing Secure Software

Section 4(e) of the Cyber EO requires NIST to issue guidance identifying practices that enhance the security of the software supply chain, including standards, procedures, or criteria regarding secure software development environments and providing "artifacts" that demonstrate conformance to such standards, processes, or criteria. Pursuant to Section 4(e), NIST released a draft Secure Software Development Framework (Draft SSDF) at the end of September 2021. The Draft SSDF bears the title Draft NIST Special Publication 800-218, Version 1.1, and consists of a core set of high-level secure software development practices that can be integrated into software development life cycles. The Draft SSDF requests comments by November 5, 2021, including responses to the questions "What types of artifacts and evidence can be captured, documented, and shared publicly as byproducts of implementing the secure software development practices?" and "Are there examples [of such artifacts and evidence] you can share?"

On October 28, 2021, NIST announced that it would hold a virtual workshop on November 8, 2021 to solicit input about the types of artifacts of secure software development that software producers can share publicly with software acquirers. The workshop will also cover approaches for "attesting to following specific secure software development practices." NIST will use the input gathered at this workshop to finalize the SSDF, which then will be incorporated into the guidelines for enhancing software supply chain security discussed above.

NIST Issues Three Guidance Documents on Cloud Security

On October 28, 2021, NIST issued three reports related to cloud security: (1) the Second Draft NIST Internal Report (IR) 8320, "Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases"; (2) Draft NIST IR 8320B, "Hardware-Enabled Security: Policy-Based Governance in Trusted Container Platforms"; and (3) Draft NIST Publication (SP) 1800-19, "Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments." Each of these reports provides

guidance on practices, techniques, and technologies for securing data in connection with various cloud services. NIST is accepting comments on all three reports until December 5, 2021.

November 2021 Developments Under President Biden's Cybersecurity Executive Order

By Robert Huffman, Susan B. Cassidy, Ashden Fein, Ryan Burnette & Darby Rourick on December 3, 2021

Posted in Cybersecurity, Internet of Things (IoT)

This is the seventh in a series of Covington blogs on implementation of Executive Order 14028, "Improving the Nation's Cybersecurity," issued by President Biden on May 12, 2021 (the "Cyber EO"). The first blog summarized the Cyber EO's key provisions and timelines, and the second, third, fourth, fifth, and sixth blogs described the actions taken by various government agencies to implement the EO during June, July, August, September, and October 2021, respectively. This blog summarizes the key actions taken to implement the Cyber EO during November 2021.

Although most of the developments in November were directed at U.S. Government agencies, the standards being developed for such agencies could be imposed upon their contractors or otherwise be adopted as industry standards for all organizations that develop or acquire software.

CISA Publishes Cybersecurity Incident Response and Vulnerability Response Playbooks

Section 6(a) of the Cyber EO notes that the cybersecurity vulnerability and incident response procedures currently used by Government agencies to identify, remediate, and recover from vulnerabilities and incidents affecting their systems vary across agencies, hindering the ability of lead agencies to analyze vulnerabilities and incidents more comprehensively across agencies. In order to achieve "standardized response processes," Section 6(b) of the EO requires the Cybersecurity and Infrastructure Security Agency ("CISA") to develop a standard set of operational procedures (playbook) to be used by civilian agencies in planning and conducting a cybersecurity vulnerability or incident response activity respecting their information systems. On November 16, 2021, CISA issued a document with two separate response playbooks, one for incident response and another for vulnerability response. These two playbooks are contained within a single document.

Both playbooks apply to all Federal Civilian Executive Branch ("FCEB") agency information systems used or operated by an FCEB agency, a contractor of such an agency, or another organization on behalf of such an agency. Although the playbooks do not expressly make provisions applicable to contractors and other non-FCEB organizations, CISA stated unequivocally that "[i]t is the policy of the federal government that information and communications technology ("ICT") providers who have contracted with FCEB agencies must promptly report incidents to such agencies and to CISA."

The Incident Response Playbook covers incidents that involve confirmed malicious cyber activity and for which a "major incident" (as defined by the Office of Management and Budget)

has been declared or not yet reasonably ruled out. The Incident Response Playbook provides FCEB agencies with a standard set of procedures to identify, coordinate, remediate, recover, and track mitigations from incidents affecting FCEB systems, data, and networks. The playbook also includes provisions for FCEB reporting of incidents to CISA and coordination with CISA and other agencies in responding to such incidents.

The Vulnerability Response Playbook applies to any vulnerability "that is observed to be used by adversaries to gain unauthorized entry into computing resources." The Vulnerability Response Playbook builds on CISA's Binding Operational Directive 22-01 and sets forth standard, high-level processes and practices that FCEBs should follow when responding to vulnerabilities that pose significant risk.

In announcing the Incident Response and Vulnerability Response playbooks, CISA stated that "future iterations of these playbooks may be useful for organizations outside of the FCEB to standardize incident response practices." Elsewhere in the playbooks, however, the reference to "future operations" was dropped. For example, CISA states that the playbooks are intended to strengthen cybersecurity response practices and operational procedures "not only for the federal government, also for public and private sector entities." It also encourages all critical infrastructure entities and private organizations to review the playbooks "to benchmark their own vulnerability and incident response practices." Thus, contractors and other private organizations may want to consider the standards, practices, and processes identified in the playbooks to assess whether any potential gaps may exist within their own internal policies and procedures.

NIST Issues Draft Criteria for Consumer Software Cybersecurity Labeling

Section 4 of the Cyber EO directs various federal government agencies to take certain actions to enhance software supply chain security. Section 4(s) requires the National Institute of Standards and Technology (NIST) to initiate pilot programs to educate the public on the security capabilities of software development practices and Internet of Things (IoT) devices. Section 4(t) requires NIST to identify criteria for a consumer labeling program that "shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone, and shall use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products." Pursuant to Sections 4(s) and (t), NIST released draft Criteria for Consumer Software Cybersecurity Labeling on November 1, 2021. NIST will accept comments on the draft criteria through December 16, 2021, and intends to issue a final version of the criteria by February 6, 2022, as required by Section 4(u) of the Cyber EO.

The draft issued by NIST has three primary goals: (1) establishing baseline technical criteria for a consumer cybersecurity label; (2) providing criteria for the form of the label, including how the label can represent cybersecurity-related risks and attributes, how the label can be tested for effectiveness, and how the public can be educated about the label and its meaning; and (3) describing how organizations attesting to the label determine their conformity with the label. The draft emphasizes that the criteria are not intended to describe how a cybersecurity label should be explicitly represented, and that NIST is not establishing its own labeling program for consumer software. "Rather, these criteria set out desired outcomes, allowing and enabling the marketplace of providers and consumers to make informed choices."

The draft describes the baseline technical criteria as a series of attestations, i.e., claims made about the software associated with the label. It organizes these attestations into the following categories: (1) Descriptive Attestations, such as who is making the claims in the label, what the label applies to, and how consumers can obtain other supporting information; (2) Secure Software Development Attestations, such as how the software provider adheres to accepted secure software development practices throughout the software development cycle; (3) Critical Cybersecurity Attributes and Capability Attestations, and (4) Data Inventory and Protection Attestations, including declarations concerning the data that is processed, stored, or transmitted by the software. The draft identifies specific attestations included in each of these categories. For example, the draft identifies the following five attestations within the Critical Cybersecurity Attributes and Capability Attestation category: (1) Free From Known Vulnerabilities; (2) Software Integrity and Provenance; (3) Multifactor Authentication (if applicable); (4) Free From Hard Coded Secrets; and (5) Strong Cryptography (if applicable).

Regarding the criteria for the form of the label itself, the draft identifies four different approaches: Descriptive; Binary; Graded; and Layered.

- A descriptive label provides information about the properties or features of the product without any grading or evaluation.
- A binary label (sometimes called "seal of approval") is a single, consumer-tested label indicating that the software has met the baseline standard.
- A graded (or "tiered") label identifies the degree to which the product satisfies the standard, often by use of colors (e.g., red-green-yellow) or number of icons.
- A layered label provides the consumer with the means to access additional information about the labeling program and the software's declaration of conformity.

In the draft, NIST proposes a binary label, which may be coupled with a layered approach in which a short URL (as included in Singapore's cybersecurity label) or scannable code (e.g., a QR code) on the binary label leads consumers to additional details online.

Finally, the draft defines the conformity assessment criteria for consumer software cybersecurity labeling based on the concept of a Supplier's Declaration of Conformity (SDOC). The draft includes a detailed discussion of what should be included in the SDOC and any supporting documentation.

NIST Publishes Security Guidance for Internet of Things Devices

NIST additionally published two guidance documents relating to IoT devices in November: (1) guidance relating to Establishing IoT Device Cybersecurity Requirements (NIST Special Publication (SP) 800-213) and (2) a revised IOT Device Cybersecurity Requirements Catalog (NIST SP 800-213A). The publications are targeted to information security professionals, system administrators, and others in organizations tasked with assessing, applying, and maintaining security on a system.

NIST SP 800-213 overviews areas of consideration for organizations when determining the applicable cybersecurity requirements for an IoT device. This includes considerations to help organizations:

- understand IoT device use case and cybersecurity characteristics (including use case and benefits, data implications, interactions with other system elements, and manufacturer practices);
- assess risk of IoT device impacts to systems (including by reviewing threat source, vulnerability, likelihood, and impact effects); and
- determine require IoT device cybersecurity characteristics (including selection of requirements from other resources, such as NIST SP 800-53 and the NIST Cybersecurity Framework).

NIST SP 800-213A serves as a companion document to NIST SP 800-213, and is referenced in the section of NIST SP 800-213 that addresses the determination of IoT device cybersecurity characteristics. It is organized in a similar way to other documents that contractors may be familiar with, such as NIST SP 800-171 and NIST SP 800-53, and contains controls that can be selected in the following categories:

- Device Identification;
- Device Configuration;
- Data Protection;
- Logical Access to Interfaces;
- Software Update;
- Cybersecurity State Awareness; and
- Device Security.

Although NIST SP 800-213A draws on other publications, it explicitly notes that "Controls are considered independent of their inclusion in SP 800-53B, Control Baselines for Information Systems and Organizations [800-53B], and so some controls included in the related controls list may not be in the low-, moderate-, and/or high-impact baseline."

NIST Holds Workshop on Proposed Artifacts of Secure Software Development That Software Providers Can Use in Self-Declarations and Attestations

Section 4(e) of the Cyber EO requires NIST to issue guidance identifying practices that enhance the security of the software supply chain, including standards, practices, or criteria regarding secure software development environments and providing "artifacts" that demonstrate conformance to such standards, processes, or criteria. Pursuant to section 4(e), NIST issued a draft Secure Software Development Framework (Draft SSDF) at the end of September 2021.

NIST conducted a public workshop on the Draft SSDF on November 8, 2021. The purpose of the workshop was to "solicit input about the types of meaningful artifacts of secure software development that software producers can share publicly with software acquirers," including insights on "attesting to following specific secure software development practices." The workshop included a panel on "Self-Declaration and Attestation" that included Warren Merkel, Chief of Standards Services for NIST. Mr. Merkel identified four steps of conformity

assessment: (1) identifying the requirement; (2) determining conformity to the requirement; (3) attestation of conformity; and (4) surveillance. Mr. Merkel then identified several different approaches to attestation, including self-attestation, third-party certification, and assessment by an entity approved by an accredited body. According to Mr. Merkel, the Draft SSDF does not require a particular form of attestation.

NIST plans to consider the input it received at the workshop, along with the comments submitted on the Draft SSDF and other sources, in developing the final SSDF, which will be part of the software supply chain security guidance that NIST is required to issue by February 8, 2022.

NTIA Issues Guidance Related to Software Bills of Materials

In November 2021, the National Telecommunications Information Administration ("NTIA") released two documents related to its ongoing efforts to establish standards for Software Bills of Materials ("SBOM"). The first of these documents is a two-page analysis entitled "SBOM Myths vs. Facts." NTIA states that this document is intended to help dispel "common, often sincere myths" about SBOM. The second document issued by NTIA identifies various initiatives, guidance, models frameworks, and reports that expressly or implicitly highlight the value of SBOM. NTIA states that this is not an exhaustive list, and that it is not endorsed by the NTIA working group that assembled the document.

December 2021 Developments Under President Biden's Cybersecurity Executive Order

By Robert Huffman, Susan B. Cassidy, Michael Wagner & Ryan Burnette on January 7, 2022

Posted in Cybersecurity, Uncategorized

This is the eighth in a series of Covington blogs on implementation of Executive Order 14028, "Improving the Nation's Cybersecurity," issued by President Biden on May 12, 2021 (the "Cyber EO"). The first blog summarized the Cyber EO's key provisions and timelines, and the second, third, fourth, fifth, sixth, and seventh blogs described the actions taken by various government agencies to implement the EO from June through November 2021. This blog summarizes the key actions taken to implement the Cyber EO during December 2021. Although the actions described below implement different sections of the Cyber EO, each of them portends further actions in February 2022 that are likely to impact government contractors, particularly those who provide software products or services to federal government agencies.

The FAR Council Announces Proposed Rulemakings in February 2022 To Impose Cyber Incident Reporting Requirements on Certain Federal Contractors and to Standardize Common Cybersecurity Contractual Requirements Across Federal Agencies

The Federal Acquisition Regulatory Council updated its regulatory agenda on December 20, 2021 to provide further information on two Federal Acquisition Regulation (FAR) cases previously established to implement various sections of the Cyber EO. The first of these updates indicated that a Notice of Proposed Rulemaking (NPRM) will be issued around February 2022 to amend the FAR to "increase the sharing of information about cyber threats and incident information between the Government and certain providers" pursuant to Office of Management and Budget recommendations under sections 2(b)-(c) and Department of Homeland Security recommendations under section 8(b) of the Cyber EO. This NPRM will also seek comment on amendments to the FAR pursuant to section 2(g)(i) of the Cyber EO to require certain contractors to report cyber incidents to the Government.

The updated regulatory agenda describes a second NPRM, also to be issued in February 2022, that will "standardize common cybersecurity requirements across Federal agencies for unclassified information systems, pursuant to Department of Homeland Security recommendations in accordance with sections 2(i) and 8(b) of" the Cyber EO. The updated agenda provides for the close of comments on both NPRMs around April 2022. The agenda provides no date for promulgation of final rules in either rulemaking, nor does it address the extent to which either rulemaking would modify or replace the cybersecurity safeguarding and reporting requirements currently applicable to most Department of Defense (DoD) contractors under Defense FAR Supplement (DFARS) 252.204-7012.

NIST and CISA Seek Input on Implementing Software Bills of Material

The National Institute of Standards and Technology (NIST) held a workshop on December 1, 2021 where, among other things, that agency sought public input on the proposed Software Bill of Materials (SBOM) requirements identified in Appendix F to the second draft of NIST Special Publication 800-161, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, Rev. 1." Appendix F describes SBOMs as an "emerging software supply chain concept," and defines an SBOM as a "formal record containing the details and supply chain relationships of various components used in building software, similar to food ingredient labels on packaging." The intent of the SBOM is to "provide increased transparency, provenance, and speed at which vulnerabilities can be identified and remediated by departments and agencies." Appendix F identifies certain SBOM capabilities that federal government agencies should require their suppliers to demonstrate. NIST representatives intend to use the input from the December 1 workshop in revising the SBOM requirements in a further draft of Appendix F that they plan to release in February 2022.

The Cybersecurity and Infrastructure Security Agency held a two day "SBOM-a-rama" virtual event on December 15 and 16, 2021, in which it sought stakeholder feedback on its efforts to build on SBOM publications by the National Telecommunications and Information Administration (NTIA). These publications include guidance on SBOM minimum requirements issued by NTIA pursuant to the Cyber EO and SBOM playbooks for software suppliers and users that NTIA issued in November 2021. NIST representatives have stated that they intend to consider the NTIA publications in fashioning the SBOM requirements in the final version of Appendix F of NIST SP 800-161.

NIST Holds Workshop On Draft Criteria for Consumer Software Security Labelling and IOT Device Labelling Pilot Programs

NIST held a workshop on December 9, 2021 to receive additional input on the draft criteria that it issued in November 2021 for the consumer software security labelling and consumer Internet of Things (IOT) devices labelling pilot programs required by the Cyber EO. Under the Cyber EO, NIST is required to issue final labelling criteria for these pilot programs by February 6, 2022. NIST intends to use the input from the December 9 workshop and other stakeholder comments in developing the final labelling criteria. NIST labeling requirements will not be mandatory at the outset, but some software manufacturers may see commercial advantages to adopting security labels voluntarily.