ACQUISITION PLANNING

CONTRACT MANAGEMENT
www.ncmahq.org
JANUARY 2024

Common Language Adopters Are Elevating the Profession

As a skilled profession, contract management has developed complex terminology over many years. NCMA's common language aligns this terminology and early adopters are elevating the future of the profession.

NCMA
NATIONAL CONTRACT MANAGEMENT ASSOCIATION
CONNECTING TO CREATE WHAT'S NEXT

COMPETENCIES A.1 B.2 B.5 1.4

Solarwinds Whips Up a Software Cybersecurity Storm

Supply chain hack brings on stringent federal software cybersecurity compliance.

By Michael G. Gruden, Evan D. Wolff, Maida Lerner, Jake Harrison, and Alexis Ward

When Russian hackers inserted malware into a SolarWinds' network monitoring software update, as many as 18,000 government and industry users were breached. The resulting stringent U.S. cybersecurity regime has federal buyers and sellers scrambling.

Here's how the 2020 SolarWinds supply chain attack spawned the federal Secure Software Development Framework (SSDF).

SolarWinds is the developer of Orion, a software that allows users to remotely administer and update IT systems, devices, and other components. Through Orion, information technology departments can essentially monitor their whole network from a single screen.

From a threat actor's perspective, Orion presented a strategic attack vector due to its network access. At the time of the SolarWinds attack, Orion was used by thousands of entities, including many Fortune 500 companies and multiple federal agencies.

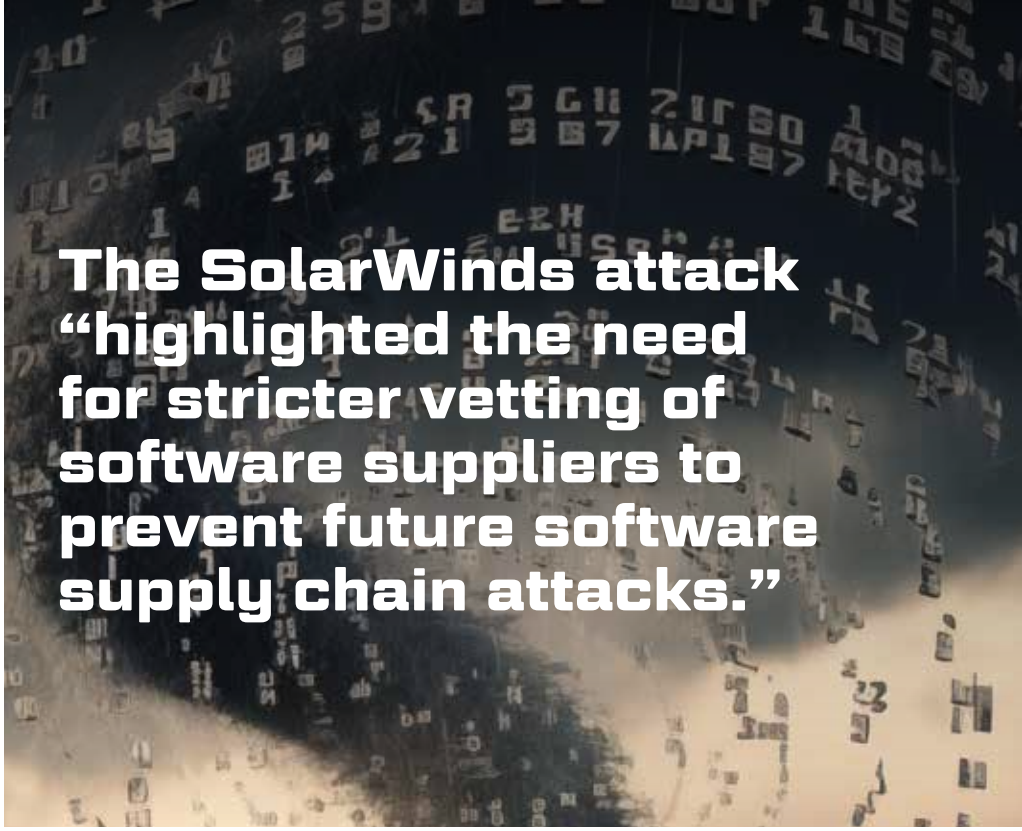
In late 2019, Russian threat actors exploited a vulnerability in SolarWinds' network to access the Orion code repository. In February 2020, after months of careful planning, the threat actors struck. Malware, known as SUNBURST, was inserted into a routine software update that SolarWinds then pushed to its customers. When activated, SUNBURST creates "backdoors" that allow third parties to enter a software ecosystem without permission.

The threat actors were careful to avoid detection. They established a command-and-control server, which enables an attacker to send commands to affected systems. The attacker would mimic the names of real systems, making detection nearly impossible. Malicious code was then inserted into SolarWinds' software code at the last possible moment before software updates went live.

SUNBURST was inherently difficult to detect as it could lay dormant for extended periods of time, even years, before going active. Moreover, the threat actor had access to thousands of computers – far more access than it used. The magnitude and duration of access to affected systems created an unparalleled opportunity for the supply chain attack.

Once users deployed the infected Orion software update, the malware allowed the threat actors to access users' environments. SolarWinds estimated that as many as 18,000 users downloaded the affected software update.[1] The threat actors compromised industry as well as federal agencies, including the Energy, Commerce, and Homeland Security departments.[2]

Making matters worse, the incidents were not uncovered for months, allowing the threat actors to run amuck within networks, doing untold damage. This unfettered access may have allowed threat actors to compromise entities that did not use any SolarWinds products but were connected to Orion users through the software supply chain.[3]



The 2020 SolarWinds attack exposed serious deficiencies in software supply chain security practices. Malicious actors were able to infiltrate a trusted software provider, insert malware into its software update, and compromise the systems of hundreds of users. Federal government networks vital to national security interests were potentially included.

This supply chain incident illustrated the risk of relying on third-party software without robust security checks. It also highlighted the need for stricter vetting of software suppliers to prevent future software supply chain attacks. Recognizing these deficiencies, the federal government began developing the Secure Software Development Framework.

Executive Order 14028

In May 2021, the Biden Administration issued Executive Order (EO) 14028 Improving the Nation's Cybersecurity, aimed at invigorating the federal government's cybersecurity defense posture. President Biden's stated goal for directing procurement and acquisition changes for federal contractors and suppliers was for the government to lead the private sector toward improved security standards and performance. As a result, the order directed the government to adopt a wide range of recommendations, rules, and standards.

At the time, there was no consistent guidance standardizing how companies should address their software supply chains. Biden's order mandated improvements in software supply chain security and integrity, placing a high priority on addressing "critical software." Importantly, it addressed supply chain vulnerabilities, noting that commercial software often lacked both transparency and the corresponding security controls necessary to defend against malicious threat actors.

The order cited a need for rigorous mechanisms to ensure software products performed securely. Federal agencies were tasked with developing guidelines and criteria to evaluate software security, including practices aimed at software developers and suppliers of products containing software.

OMB Memorandum M-22-18

In response to EO 14028, the Office of Management and Budget (OMB) published OMB Memorandum M-22-18 ("M-22-18")[4] on September 14, 2022. M-22-18 generally requires federal agencies to ensure that their software suppliers comply with the National Institute of Standards and Technology (NIST) Software Supply Chain Security Guidance and NIST Special Publication (SP) 800-218 (collectively, the "NIST Guidance"), which were developed in February 2022.

M-22-18 does not apply to all software developed by federal software vendors. Instead, it applies to third-party software that a federal agency uses on agency information systems or in a way that otherwise affects the agency's information. M-22-18 is not retroactive; it applies only to agencies' use of software developed or modified by major version changes after September 14, 2022.

"Software" subject to M-22-18 is defined broadly to include firmware, operating systems, applications, and application services (e.g., cloud-based software), and products containing software. OMB has not defined "products containing software." However, government suppliers should be prepared to comply with M-22-18 even when selling products to the government that are not normally thought of as software but are products sold with software included, such as computers, printers, etc.

NASA **SEWP**

Solutions for Enterprise-Wide Procurement

VISIT THE NASA SEWP BOOTH AT

AFCEA WEST 2024!

San Diego, CA

February 13-15

Booth #2716

Scan the QR code to register

(301) 286-1478
help@sewp.nasa.gov

M-22-18 directs agencies to ensure compliance by collecting self-attestation forms from their third-party software suppliers. The Cybersecurity and Infrastructure Security Agency (CISA) published a draft standard attestation form for agency use. A final attestation form was expected to be released in Fall 2023, but had not as of mid-October. The CISA attestation form generally asks suppliers of in-scope software to confirm that they comply with the NIST Guidance throughout the software development life cycle.

As an alternative to self-attestation, M-22-18 allows suppliers to provide a third-party assessment performed by either a certified FedRAMP Third Party Assessor Organization (3PAO) or an assessor approved by the agency, so long as the assessor uses the NIST Guidance as the assessment baseline.

In addition to assessments, an agency can also require software suppliers to submit a software bill of materials (SBOM) if the software is "critical software" as defined in OMB Memorandum M-21-30 ("M-21-30"), or if the agency otherwise determines that an SBOM is necessary.[5]

"Critical software" is defined in M-21-30 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
- Operates outside of normal trust boundaries with privileged access."

The original attestation deadlines included in M-22-18 were superseded by OMB Memorandum M-23-16, published in June 2023, and no longer apply. It is nonetheless crucial that software suppliers determine whether the software they supply to the government may be categorized as "critical software."

OMB Memorandum M-23-16

In OMB Memorandum M-23-16 ("M-23-16"), released in June 2023, OMB extended the deadline for agencies to collect attestations of compliance from software developers.[6] The new deadlines now depend on the final publication of the attestation form. Agencies must now collect attestations three months after finalization of the form for critical software and six months for all other software.

The M-23-16 definition of "critical software" for purposes of the attestation submittal deadline is the same as the M-21-30 definition above. The critical software definition applies only to production software, not testing or research software.

M-23-16 also lays out guidance regarding the use of plans of action and milestones (POAMs) for times that developers are unable to attest to compliance with the NIST guidance. Developers must specifically identify the controls to which they are unable to attest, document practices they have in place to mitigate risks, and submit the POAM to the agency. If the agency determines the POAM is satisfactory, a developer may seek an extension deadline for attestation from OMB. Without a satisfactory POAM and extension, the agency must discontinue use of the software.

CISA Draft Attestation Form

In April 2023, CISA released its draft Secure Software Development Self-Attestation Form. The form lays out the minimum security requirements that software developers will be required to meet. Additionally, agencies may supplement the CISA requirements with additional agency-specific requirements that must be approved by OMB before implementation.

The draft form specifies that attestations are required for all software developed after September 14, 2022, any existing software that is modified by a major version change after September 14, 2022, and any software that has continuous delivery or deployment of code.

Attestations are not required for software developed by federal agencies or any software freely obtained by an agency, such as freeware or open source software. Additionally, as an alternative to self-attestation, developers may obtain compliance certification by a FedRAMP third-party assessor organization (3PAO), as mentioned above.

The self-attestation form includes four core secure development areas based on the security requirements in EO 14028 and the NIST SSDF. These areas include developing software in secure environments, maintaining trusted source code supply chains, maintaining data provenance for internal and third-party code incorporated in the software, and employing automated tools or comparable processes that identify

security vulnerabilities. The form cites specific NIST SP 800-218 controls and guidance, which allows developers to begin assessing readiness ahead of the attestation deadline.

NIST SP 800-218 Overview

Integral to compliance with OMB Memoranda M-22-18 and M-23-16 is implementation of NIST SP 800-128, *Secure Software Development Framework (SSDF)*. NIST SP 800-218 (February 2022) includes 42 controls (or "tasks") broken out across four families of controls: Protect the Organization (PO), Protect the Software (PS), Produce Well-Secured Software (PW), and Respond to Vulnerabilities (RV).

The controls are designed to guide entities from beginning to end of the software development life cycle (SDLC). The controls are written with a focus on achieving a certain outcome; the tools and techniques used to get there are left to the implementing entity. A few controls stand out as particularly notable.

RV.1.3 requires developers to "have a policy that addresses vulnerability disclosure and remediation, and implement the roles, responsibilities, and processes needed to support that policy." Developing a comprehensive policy from scratch isn't easy, and, per RV.2.2, company policies need to include a specific risk response plan for any vulnerability identified.

PO.5 requires developers to "implement and maintain secure environments for software development." Companies will need to ensure their development environments are secure through several measures. These include implementing multifactor authentication (MFA) on development servers, building Federal Information Processing Standards (FIPS)-validated cryptography and full disk encryption for endpoints into SDLC processes, and employing least privilege by removing any unnecessary access or administrative capabilities from endpoints.

PS.1 requires developers to "protect all forms of code from unauthorized access and tampering." This will include restricting access to code repositories based on nature of code as well as implementing version control features to track all changes with accountability to individual accounts. Code owners will also need to review and approve all changes made to code by others.

PS.3 directs developers to "archive and protect each software release." To do this, companies will need to develop a software bill of materials. The SBOM will need to include all dependencies, libraries, and external functionality on which software relies. It will also need to include the source and version of all included items. Companies will then need to avoid or remediate security incidents for these documented items.

The SBOM is a new concept rooted in how the government manages its bill of materials (BOM) for software. The importance of an SBOM lies in its ability to itemize all software components utilized, including licenses, versions, and patches, so that the government can identify any associated risks.

PW.4 requires developers to "reuse existing, well-secured software when feasible instead of duplicating functionality." Developers will need to obtain data provenance information and SBOM information for any commercial software used to be able to fully understand and assess associated risk. Developers may want to establish a repository of vetted commercial options and should have formal patching and updating processes for commercial software.

Finally, under PW.5, developers must "create source code by adhering to secure coding practices." This will require developers to standardize the style and formatting of source code. They will also have to review their own code in addition to seeking code review by other people or tools. Developers must also use development environments with automated features that encourage or require the use of secure coding practices.

Companies will need to think ahead in order to fully comply by OMB's deadlines.

Software Supply Chain Roadmap: Top 5 Action Items

Even though the *Federal Acquisition Regulation* (*FAR)* Council has an open *FAR* case[7] to implement section 4(n) of EO 14028 requiring software attestations, contractors will need to comply with the SSDF requirements prior to the *FAR* rule finalization. The reason is, federal agencies are creating their own requirements concurrent with CISA's finalization of the self-attestation form.

Regardless of where companies are on the road to software supply chain security compliance, there are several steps they can take now to ensure they meet the SSDF requirements and OMB memoranda.

1. Establish a corporate software compliance team that includes

legal, software development, and leadership stakeholders. We often refer to cybersecurity as a team sport meaning it requires more than a software developer or contracts manager to implement the emerging SSDF requirements. Ultimately, it requires buy-in and support in time and resources from executive leadership as well as the general counsel and chief information security officer (CISO). The more stakeholders around the figurative table in discussing SSDF compliance, the greater likelihood there will be support throughout the organization and effective implementation.

2. Review the NIST SP 800-218 practices and tasks as well as the draft self-attestation form.
3. Review guidance to determine whether any software an organization develops could be viewed as "critical." Every company should be confident whether or not its software at issue is "critical" because this determination will dictate the company's compliance deadline. A requirement to implement and attest to the SSDF three months sooner than other software producers could have a significant impact on refining a company's compliance posture. Therefore, companies should be certain whether or not they need to meet the earlier requirements.
4. Engage an independent third party, preferably under legal privilege, to complete a NIST SP 800-218 assessment of the organization's SDLC and development environment. NIST SP 800-218 validation is likely most effective when conducted by an external third-party and under attorney client privilege. Using counsel with technical capabilities to conduct the assessment or to direct the assessments by third parties under the protections of attorney client privilege can benefit companies if needed to demonstrate to customers and the government that an independent assessment was conducted and also to mitigate the risk of having to disclose assessment findings in litigation or during an investigation.
5. Develop a plan of action and milestones for any identified gaps.

Conclusion

It is still uncertain where the new *FAR* clause and OMB's guidance will lead. However, companies can take the steps outlined to navigate toward software supply chain security compliance. **CM**

Michael G. Gruden, a counsel at Crowell & Moring LLP's Washington, D.C. office, is a former Pentagon Information Technology Acquisition Branch Chief and a leading cybersecurity lawyer who helps government contractors navigate privacy, cybersecurity, and contract compliance requirements. Drawing from his experience at the U.S. Department of Defense and U.S. Department of Homeland Security, Gruden represents some of the nation's largest defense contractors and tech companies as they prepare to meet CMMC requirements and mitigate cyber threats. He can be reached at mgruden@crowell.com.

Evan D. Wolff is a partner in Crowell & Moring's Washington, D.C. office where he helps lead the Privacy & Cybersecurity practice. With a national reputation for his deep technical background and understanding of complex cybersecurity legal and policy issues, Wolff represents numerous critical infrastructure companies, trade organizations, and the nation's largest defense contractors. He can be reached at ewolff@crowell.com.

Maida Lerner is senior counsel in Crowell & Moring's Washington, D.C. office and part of the firm's Privacy & Cybersecurity and Government Contracts groups. She advises clients across a variety of sectors including government contracts, pipeline, transportation, health care, and manufacturing, in the areas of cybersecurity and privacy compliance. She can be reached at mlerner@crowell.com.

Jake Harrison is an associate in Crowell & Moring's Washington, D.C. office. Harrison counsels government contractors on compliance and regulatory issues with a focus on cybersecurity and data privacy compliance. He can be reached at jharrison@crowell.com.

Alexis Ward is an associate in Crowell & Moring's Los Angeles office where she is a member of the Privacy & Cybersecurity and Government Contracts groups. She can be reached at award@crowell.com.

ENDNOTES

1 See Form 8-K SolarWinds Corporation Current Report, Sec. & Exch. Comm'n (Dec. 14, 2020), https://www.sec.gov/Archives/edgar/data/1739942/000162828020017451/0001628280-20-017451.txt (Document No. 0001628280-20-017451).
2 See David E. Sanger, Russian Hackers Broke into Federal Agencies, U.S. Officials Suspect, N.Y. Times (updated May 10, 2021), https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html.
3 See Marcin Kleczynski, Malwarebytes Targeted by Nation State Actor Implicated in SolarWinds Breach, Malwarebytes Blog, https://www.malwarebytes.com/blog/news/2021/01/malwarebytes-targeted-by-nation-state-actor-implicated-in-solarwinds-breach (last updated Jan. 27, 2021).
4 https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security.pdf
5 https://whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf
6 https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security.pdf
7 FAR Case 2023–002, Supply Chain Software Security.