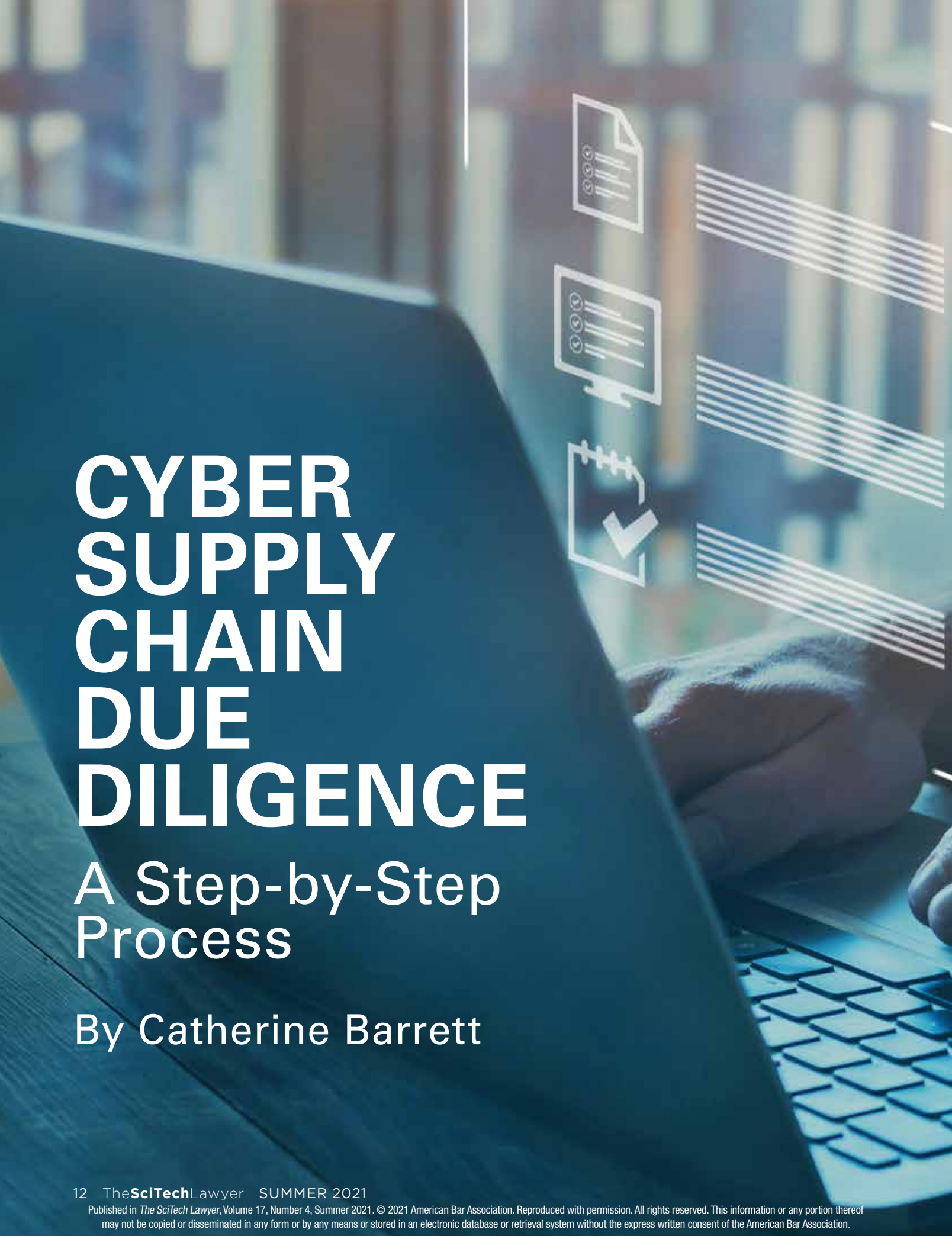

CYBER SUPPLY CHAIN DUE DILIGENCE

A Step-by-Step Process

By Catherine Barrett

Image: anyaberkut/iStock / Getty Images Plus via Getty Images

The announcement in December 2020 of the SolarWinds supply chain attack brought international attention to what Brad Smith, president of Microsoft, characterized as a "notable attack for both the scale and scope" during his testimony before the Senate Select Committee on Intelligence on February 23, 2021.[1] He testified that Microsoft estimated approximately 1,000 engineers worked on the SolarWinds attack, which he described as an advanced persistent threat (APT)[2] carried out by Russia.[3] The attackers penetrated a SolarWinds "network and applications monitoring platform called Orion" and included "trojanized updates" as part of the normal patching process, prompting SolarWinds Orion users to unwittingly download the malware as part of the normal security patching process.[4] According to the U.S. government, which characterized the attack as "an intelligence gathering exercise," approximately 18,000 public and private sector organizations were compromised by this attack.[5] While the investigation to identify how the foreign adversary gained initial entry into SolarWinds is ongoing, the supply chain attack highlights the need for organizations, both public and private, to adopt a comprehensive, sophisticated approach to cyber supply chain due diligence.

According to the National Institute of Standards and Technology (NIST), Information and Communications Technology (ICT) supply chain risks may include "insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the ICT supply chain."[6] Whether purchasing or licensing ICT to support operations or manufacturing/supplying ICT, organizations need visibility into their supply chain to manage risk, to understand how and where ICT is being "developed, integrated, and

EXAMPLE BENCHMARK AND ACCOMPANYING DUE DILIGENCE QUESTIONS

	KEY PRACTICES FOR C-SCRM[12]	DUE DILIGENCE
GOVERNANCE	Integrate C-SCRM across the organization by establishing supply chain risk councils that include executives from supply chain/procurement, information technology (IT), cybersecurity, operations, legal, enterprise risk management (ERM), and other functional and leadership areas of the organization to regularly review risk and mitigation plans, set priorities, direct sharing of best practices, and pilot initiatives.	• Does the supplier/vendor integrate C-SCRM across its organization? • Does the supplier/vendor consider supply chain risk via a formally established council or body with representatives from across the business? • Is leadership and/or the executive board monitoring C-SCRM, including threshold of risk tolerance and performance measures? • Are supplier/vendor supply chain security roles and responsibilities articulated in agreement/contract for goods/services?[13]
	Develop a C-SCRM plan and establish a formal C-SCRM program to ensure organizational accountability for managing cyber supply chain risk.[14] "Mature organizations have formal programs with established governance, policies and procedures, processes and tools."[15]	• Does the supplier/vendor have a C-SCRM plan? • Does the supplier/vendor have a C-SCRM program? • Does the supplier/vendor have C-SCRM policies, procedures, and practices that align to applicable federal and state laws, regulations, and guidance? • Are roles and responsibilities of program participants documented via policies and/or procedures? • Are procedures in place to facilitate implementation of C-SCRM policies and procedures? • Are C-SCRM requirements integrated into the acquisition/procurement life cycle?
	Designate a leader to organize, develop, and manage C-SCRM program, policies, and procedures and ensure they are regularly reviewed and updated.[16]	• Does the supplier/vendor have a designated lead to organize, develop, and manage its C-SCRM program?
	Understand and monitor supply chain, including components. To manage cybersecurity risk emanating from supply chains, organizations must understand their own supply chains and those of their suppliers/vendors too.	• Can the supplier/vendor demonstrate real-time identification and monitoring of its supply chain? • Does the supplier/vendor have access to an organization's IT infrastructure, including cloud and/or data?
	Compile list monitoring suppliers experiencing C-SCRM-related issues, indicating heightened risk/caution.[17]	• Is the supplier/vendor in good standing?
	Establish remediation criteria to address identified C-SCRM-related issues to move supplier/vendor off list and into good standing.	• Has the supplier/vendor complied with established remediation criteria, if applicable?
	Include critical suppliers, products, and assets in contingency planning, incident response, and disaster recovery.[18]	• Is the supplier/vendor a critical supplier to the organization? • If so, are the responsibilities of being a named critical supplier to the organization documented in writing and understood by the supplier/vendor? • Does the supplier/vendor have its own contingency plan, incident response plan, and disaster recovery plan?
	Establish a process to mentor/coach suppliers/vendors on C-SCRM practices, performance metrics, audit, and approach to making required improvements.	• Does the supplier/vendor comply with established mentorship/coaching process?
	Test contingency plans, incident response plans, and disaster recovery plans with key stakeholders, including suppliers, to ensure readiness, relevance, and efficacy of the plans[19]	• Does the supplier/vendor understand and accept responsibilities associated with testing contingency, incident response, and disaster recovery plans? • Does the supplier/vendor have the resources required to address gaps found from the testing process? • Does the supplier/vendor test its own contingency, incident response, and disaster recovery plans on a regular basis?

	KEY PRACTICES FOR C-SCRM[12]	DUE DILIGENCE
GOVERNANCE	Identify and manage critical suppliers that, if disrupted, would result in negative business impacts on the organization. Critical suppliers are also those that provide mission-critical components (products or services) that support the organization.[20]	• Does the supplier/vendor identify and manage its critical suppliers? • Has the organization diversified suppliers/vendors, building relationships with others likely to be unaffected by disruption?[21]
	Establish a process to validate the integrity of internal systems and components, data, and provenance of technology, products, and service (pedigree).[22]	• Does the supplier/vendor have a process to collect, verify, and track authoritative information regarding point of origin and changes to internal systems and components, data technologies, products, and/or services?
	Establish supplier/vendor monitoring program covering the entire supplier/vendor life cycle to actively track a variety of risks, including security, privacy, quality, financial, and geopolitical, among others.[23]	• Does the supplier/vendor meet cybersecurity and other agreed-upon requirements?
	Review data to identify any change in supplier/vendor status (e.g., financial legal or ownership).	• Does the supplier/vendor provide notice of change in status to organization?
	Audit and assess supplier/vendor controls regularly to manage cyber supply chain risks, determine whether agreed-upon requirements and controls are met, identify required improvements, and monitor completion of those improvements.	• Does the supplier/vendor cooperate fully, in a timely manner, and in good faith with audit and assessment of cyber supply chain risks, requirements, controls, and subsequent improvements?
	Engage outside third parties regularly to conduct authorized, unannounced information security assessments. Assessments may include testing, examination, and interviewing.[24]	• Does supplier/vendor engage outside third parties to conduct information security assessments?
	Establish agreements and procedures with suppliers/vendors for notification of supply chain compromises and potential compromises and results of assessments or audits.	• Does the supplier/vendor have an established notification process for supply chain compromises, potential compromises, and results of assessments or audits?

deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services."[7] Undetected vulnerabilities within an organization can be exploited by malicious actors, causing direct and indirect financial, reputational, and legal harm, among other issues, to the organization.

To mitigate potential cyber supply chain risk, organizations need to perform due diligence prior to entering into a partnership and then thereafter, on a continual basis. Due diligence (in this context) refers to a process used to identify cyber risk associated with third-party suppliers/vendors.[8] The process should be one that a reasonably prudent person would be expected to perform, a process that references commonly used industry standards, guides, and practices for cyber supply chain risk management. In this article, the due diligence step-by-step process incorporates references from a variety of supply chain risk management publications from the National Institute of Standards and Technology (NIST)[9] and the proposed due diligence–related questions are derived from these publications.

In the wake of the SolarWinds attack, there is growing interest for greater supply chain transparency, to gain visibility into the security of supply chains by assessing supplier/vendor risk. Also, there's interest in propagating cyber supply chain risk management (C-SCRM) contractual requirements from suppliers/vendors to sub-suppliers. C-SCRM refers to a process of "identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of [information communication technology] ICT product and service supply chains."[10]

Recognizing some U.S. industries, such as pharmaceuticals, rely heavily on foreign sources of critical materials and may, therefore, face foreign ownership, control, or influence (FOCI)-related risk (i.e., geopolitical), where possible, organizations are considering diversification of sources for critical materials. The end result of these and other secure cyber supply chain measures could be the cancelation of agreements with suppliers and sub-suppliers that fail to meet security requirements.

CYBER SUPPLY CHAIN DUE DILIGENCE STEP-BY-STEP PROCESS

A recent World Economic Forum report noted, "supply-chain attacks can tear through increasingly interconnected companies, passing from vendor to partner, and wreaking havoc on industries and economies."[11] Given the risk, conducting C-SCRM due diligence prior to engaging prospective suppliers/vendors is both a reasonable and necessary step to mitigate risk.

Identify benchmark(s)

- Determine objectives of the due diligence exercise; this, in turn, will help guide the benchmark selection.
- Benchmarks may include one or more of the following sources: laws, regulations, governmental guidance, industry association,

or standards organization, among others.
- Compile a list of secure cyber supply chain requirements from one or more sources to comprise the benchmark.

Draft questions from benchmark

- Formulate questions derived from the list.

Screen suppliers

- Apply questions to each prospective supplier/vendor to identify potential risks.
- Verify information provided by the supplier with independent research and analysis.

Assess risk of suppliers

- Assess risk of supplier/vendor within the context of the organization's established risk threshold.
- Determine whether prospective supplier/vendor risk should be accepted, mitigated, or avoided.
- Determine whether to enter into a partnership with the supplier/vendor.
- Determine method(s) and timeline for C-SCRM continuous monitoring of supplier/vendor.

CONCLUSION

The example benchmark and due diligence questions highlight the importance of prudent inquiry, of "taking a look under the hood" prior to entering into a partnership with a supplier/vendor. Like any partnership, it is important to stay engaged, to maintain situational awareness in order to identify any changes in status that might give rise to C-SCRM-related threats. This constant vigilance can be aided by technology, but active and informed leadership is required to manage C-SCRM-related risk.

*Catherine Barrett is a cyber policy principal with MITRE in McLean, Virginia. She is the author of "Emerging Trends from the First Year of EU GDPR Enforcement" and "Are the EU GDPR and the California CCPA Becoming the De facto Global Standards for Data Privacy and Protection?" (*The SciTech Lawyer *Spring 2020 and Spring 2019, respectively) and the co-author of the book* What Is . . . Telemedicine? *(ABA, 2015). She received her JD/MBA from the American University Washington College of Law and is a (ISC)2 Systems Security Certified Practitioner (SSCP).*

Approved for Public Release PRE 21-01058. Distribution Unlimited. The author's affiliation with The MITRE Corporation is provided for identification purposes only and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.

ENDNOTES

1. Select Comm. on Intelligence, *Hearing on the Hack of U.S. Networks by a Foreign Adversary* (Feb. 23, 2021), https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary.

2. The National Institute of Standards and Technology defines "advanced persistent threat" as

> an adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.

See Glossary: advanced persistent threat (APT), Nat'l Inst. of Standards & Tech., Computer Sec. Res. Ctr., https://csrc.nist.gov/glossary/term/advanced_persistent_threat (last visited Mar. 31, 2021).

3. Press Release, White House, FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government (Apr. 15, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government. *See also* Select Comm. on Intelligence, *supra* note 1.

4. Lucian Constantin, *SolarWinds Attack Explained: And Why It Was So Hard to Detect*, CSOonline.com (Dec. 15, 2020), https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html.

5. Press Release, Cybersecurity & Infrastructure Sec. Agency, Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA) (Jan. 5, 2021), https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

6. Jon Boyens et al., Nat'l Inst. of Standards & Tech., Supply Chain Risk Management Practices for Federal Information Systems and Organizations, SP 800-161 (Apr. 2015), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf. Implementing a tamper protection program, including antitamper technologies, may provide protection for systems, system components, and/or system services against threats, "including reverse engineering, modification, and substitution." *See* Nat'l Inst. of Standards & Tech., Security and Privacy Controls for Information Systems and Organizations, SP 800-53, Rev. 5 (Sept. 2020), https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final [hereinafter NIST SP 800-53, Rev. 5].

7. Boyens et al., *supra* note 6.

8. *Black's Law Dictionary* defines "due diligence" as "a measure of prudence, activity, or assiduity, as is properly to be expected from, and ordinarily exercised by, a reasonable and prudent man under the particular circumstances; not measured

by any absolute standard, but depending on the relative facts of the special case. *See What Is Due Diligence?*, The Law Dictionary, https://thelawdictionary.org/due-diligence (last visited Mar. 31, 2021).

9. The National Institute of Standards and Technology (NIST) researches supply chain risk management and publishes guides, research findings, tools, case studies, briefing papers, and other resources via the NIST Cyber Supply Chain Risk Management site: https://csrc.nist.gov/projects/cyber-supply-chain-risk-management (last visited Mar. 30, 2021).

10. *Cyber Supply Chain Risk Management*, Nat'l Inst. of Standards & Tech. (Apr. 2, 2021), https://csrc.nist.gov/projects/cyber-supply-chain-risk-management.

11. World Economic Forum, Principles for Board Governance of Cyber Risk (Mar. 2021), https://www.weforum.org/reports/principles-for-board-governance-of-cyber-risk.

12. Key practices in cyber supply chain risk management are compiled from NISTIR 8276, *infra* note 13, and analysis of NIST SP 800-53, Rev. 5, *supra* note 6.

13. Service level agreements (SLAs) may be used to establish requirements with suppliers/vendors. *See* Nat'l Inst. of Standards & Tech, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry, NISTIR 8276 (Feb. 2021), https://csrc.nist.gov/publications/detail/nistir/8276/final [hereinafter NISTIR 8276].

14. For an overview of SCRM plan controls, see NIST, SP 800-53, REV. 5, *supra* note 6.

15. NISTIR 8276, *supra* note 13. To review a list of high-level characteristics of a formal C-SCRM program, including proper disposal of data, documentation, tools, systems components, and other features of a formal C-SCRM program, refer to page seven of the NISTIR 8276 and NIST SP 800-53 Rev. 5, Supply Chain Risk Management Controls (3.20), *supra* note 6.

16. NIST SP 800-53, REV. 5, *supra* note 6.

17. Suppliers/vendors being monitored for C-SCRM-related issues should not be used until approval from supply chain risk council or like body. See NISTIR 8276, *supra* note 13, at 13.

18. Plan should establish protocols for vulnerability disclosure, protocols for communication with external parties during and after an incident, and process for incident notification. Plans should also be updated periodically with lessons learned. *See id.*

19. *Id.* For more information about resilience and improvement activities associated with mature organizations, refer to *id.* at 10.

20. *Id.* For a list of criteria used to determine component and supplier criticality, such as whether a supplier has access to the organization's IT systems and/or network infrastructure, refer to *id.* at 8, 10.

21. Employ a diverse set of sources to supply system components and services, hardware, and software. *See* NIST SP 800-53, REV. 5, *supra* note 6, at 366.

22. *Id.*

23. NISTIR 8276, *supra* note 13. For a complete review of the merits of assessing and monitoring suppliers, refer to *id.* at 12.

24. According to NIST SP800-115, Testing is the process of exercising one or more assessment objects under specified conditions to compare actual and expected behaviors. Examination is the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence. Interviewing is the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or identify the location of evidence.

NAT'L INST. OF STANDARDS & TECH., TECHNICAL GUIDE TO INFORMATION SECURITY TESTING AND ASSESSMENT, SP 800-115 (Sept. 2008), https://csrc.nist.gov/publications/detail/sp/800-115/final.