Supply Chain Cybersecurity includes a complex of everyday operating issues affected by a network of known and unknown connections, services and components. This paper provides a strategic overview of the supply chain cyber issues from the perspective of vendor operational security.

We examine the accelerating escalation of supply chain risks, leading to 2021 executive orders and vendor cyber certification requirements. Concise recommendations and links to frameworks and self-assessment resources provide a starting point for the journey to a healthier supply chain.

Supply Chain Cybersecurity

Maria Horton, CISSP, ISSMP, IAM and Shivaji Sengupta

OVERVIEW OF SUPPLY CHAIN RISKS

The concept of supply chain is associated with the ability to effectively orchestrate multiple vendors to deliver a final product or service. The complementary adoptions of low-cost interoperable technologies, alongside rapid innovations in physical and virtual systems/applications, now comprise the core risk drivers of today's public and private sector supply chains.

The supply chain benefits of lower costs, product innovation and improved services are manifest. However, the very same tools that allow for just-in-time delivery of products and services from a variety of suppliers vastly increase the risks of potential threats and actual exploits. Traditional information technology (IT) and supply chain risks persist in the form of data loss and corruption, misconfiguration and denied access to resources. Growing threats include ransomware, the insertion of fraudulent data, unauthorized information extraction or production, tampering with products and services to impact performance, and even tracking Global Positioning System (GPS) tools attached without distorting the original function of the product or service. Whether singular, chained, simultaneous or multiple events—these cyberexploits can provoke devastating repercussions for the entity acquiring the services or products as well as end users.

Purpose

This paper seeks to build situational awareness and inform the reader of evolving cyber supply chain standards, guidelines, regulations and risk evaluation tools. The authors also provide concise recommendations and links to resources that establish a starting point toward healthier supply chain cybersecurity.

UNDERSTANDING SUPPLY CHAIN CYBERSECURITY

Supply chain cybersecurity (SCC) focuses on planning efforts and preventative actions to reduce cyber threats, exploits and data leakages across the entire supply chain, including second- and third-tier suppliers. Supply Chain Risk Management (SCRM) is a broader logistics planning effort that addresses cybersecurity risks faced in the operational setting.

Framing The Risks

Traditional IT cyber risks are primarily perceived as the loss, corruption or misconfiguration of stored data, or denied access to resources. SCC considers the additional risks of insertion of fraudulent data, unauthorized production, tampering with products or services and even tracking tools attached to or hidden within the product or service. An adjacent concern to SCC is the recent exponential growth of remote Internet of Things (IoT) sensors, such as smartphones and radio frequency identification tracking chips, which add billions of independent nodes to the edge of networks wherein these sensors and networks contribute to the supply chain.

Supply chain cyber risks are magnified by the fact that most entities have very little understanding about the technologies they acquire, or the standards used in development, integration and deployment of said on-premises and third-party technologies. Lack of SCC situational awareness and accountability makes it easier for malicious actors (nation-states, competing companies, individuals) to create sophisticated and difficult-to-detect threats and vulnerabilities. In reality, the products and services, including developer toolkits, cloud-based resources, software libraries and Enterprise Resource Planning solutions, companies have come to rely upon originate locally and abroad. An adversary might have the capability to insert malicious code into a reputable software product, or even convince a manufacturer to hand over specifications for sensitive equipment used by U.S. federal and state governments.

The critical point is that products and services might contain SCC risk vulnerabilities that are impossible to know or eliminate without concerted cyber

hygiene efforts up and down the supply chain. There could be immediate and delayed repercussions from SCC exploits on enterprise performance, customers' operations, organizational reputation, intellectual property, finances and from a legal standing. Serious understanding and control of which software, hardware or components are "safe" is difficult and requires considering more than just the immediate supplier in contact with your organization—all of which increases costs and time. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161 graphic below depicts challenges in the supply chain.

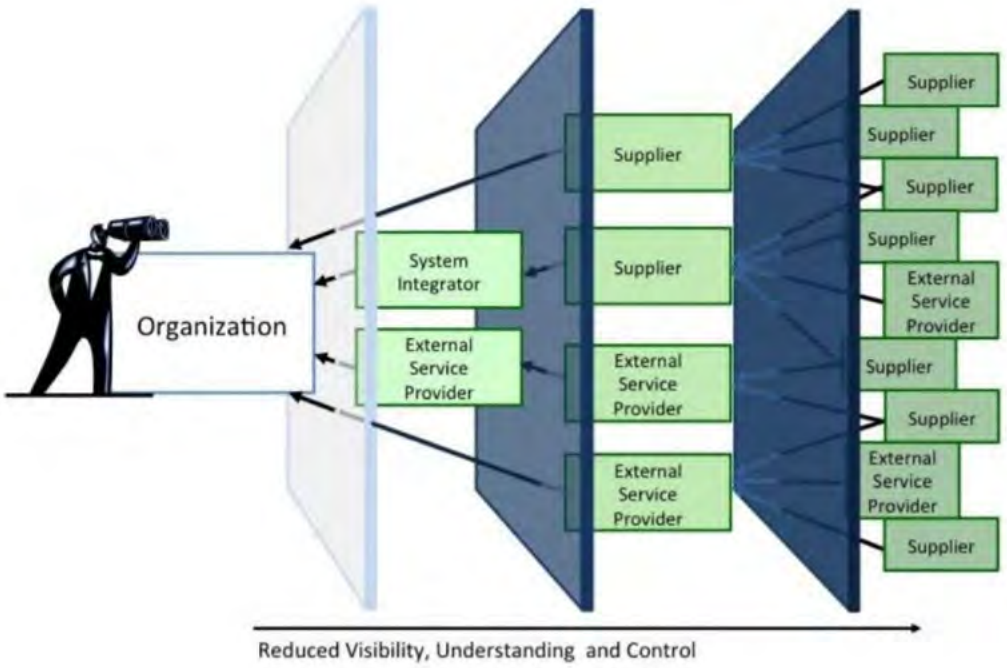
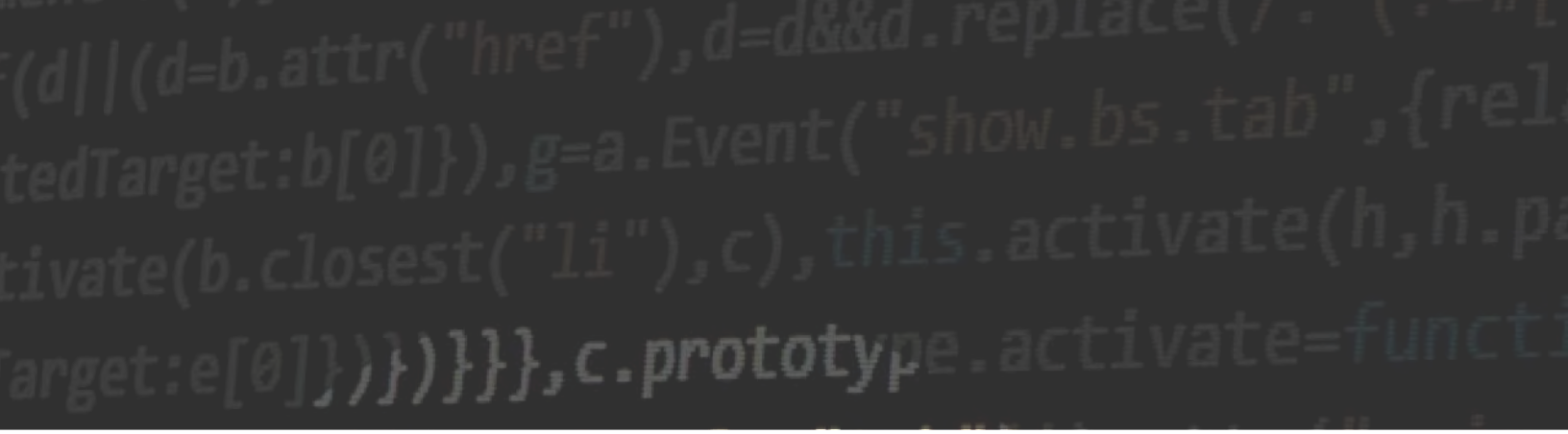


Figure- -1: NIST SCC View Demonstrates the Complexity

Adding complexity to the physical and virtual challenges of SCC is the use of multiple standards among today's entities, system integrators, external system service providers, information communications technology (ICT) and operational technology service providers. The ongoing implementation of standards, regulations, guidelines, directives and executive orders requires persistence and



creativity. Competing requirements might establish areas of overlap, conflicts and even activities that invalidate one standard while trying to implement another. The result can be increased costs, increased potential liabilities and noncompliance.

Appendix B of this paper provides a concise listing of relevant standards, regulations, guidelines, directives and executive orders that could apply to your organization depending on private, public or other applicable contracts.

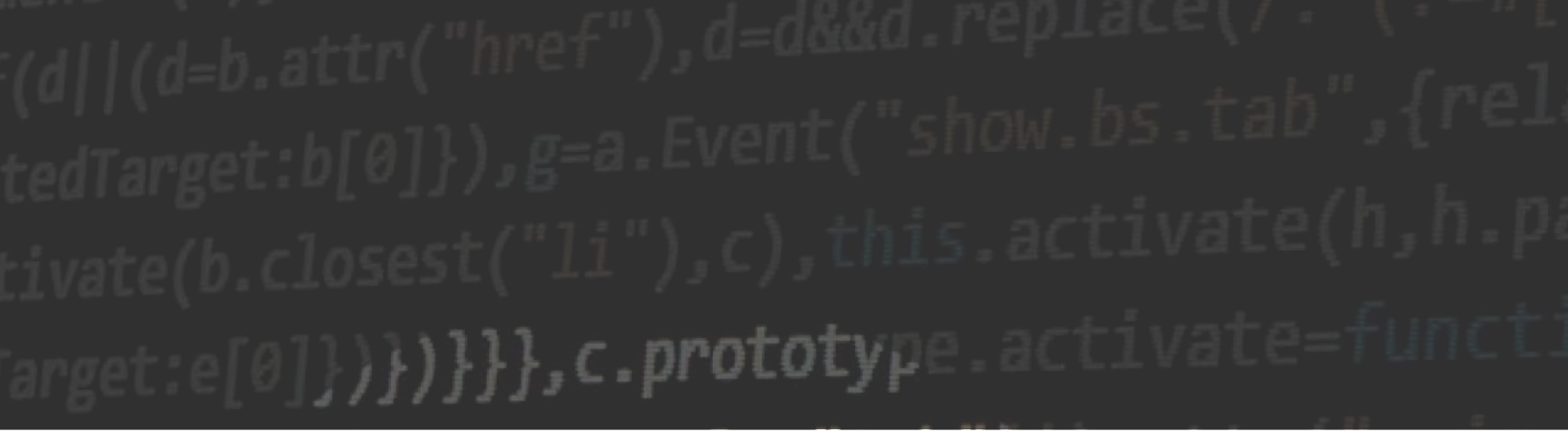
Attack Vectors and Attack Surfaces

To further understand the extent of cyber risks and vulnerabilities within the supply chain, it is important to recognize the related concepts of attack vectors and multiple attack surfaces.

Attack vectors are essentially the pathways or methods used to compromise a system, application or technology. Examples of attack vectors in operations include:

- The procurement of compromised software and hardware
- Vulnerabilities embedded in supply chain management systems
- Software security vulnerabilities in supplier systems
- The use of counterfeit hardware
- The use of hardware with embedded malware
- Compromised third-party storage or data aggregators
- Unsatisfactory information security practices by external suppliers
    - Physical third-party service providers such as janitorial services, delivery services, physical protection personnel and food services
    - Any service provider with virtual access to information, software code or the delivery of services through IT applications/reports
    - Insider threats of third-party service providers

An *attack surface* is simply the sum of all ingress points that might be used by an unauthorized attacker or exploit. A large attack surface functions as a force multiplier for the “bad guy” within the supply chain as it provides the depth and breadth of potential exploitable areas. Attack surfaces include all mobile, corporate, supplier and remote devices, including home printers and smart microphones connected to organization-owned or organization-managed assets.



CISA – Mapping Threats to Supply Chain Cybersecurity

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) lists recent examples of attacks that highlight the escalating threats organizations face throughout the supply chain.

- **Distribution**—In 2012, researchers from a major software company in the United States conducted an investigation of counterfeit software. They found malware was pre-installed on several devices. Other investigations revealed infected desktops and laptops were shipped to a distributor, then eventually to a reseller.
- **Design**— In 2016, a foreign company designed software used by a U.S. cellphone manufacturer. Evidence showed the phones made encrypted records of peoples' personal information (e.g., contact information, call history and text messages). This information was transmitted to a foreign server every three days.
- **Acquisition and Deployment**—In 2017, foreign intelligence services used an antivirus vendor based outside of the United States as a means of committing espionage on the U.S. government. Consequently, the U.S. government no longer conducted business with this vendor. Government customers also were directed to remove the vendor's products from their networks.
- **Development and Production**—In the 2020 SolarWinds incident, foreign threat actors infiltrated an IT management company, letting threat actors access the company's build server, where they modified the update process to gain access to customers' networks.

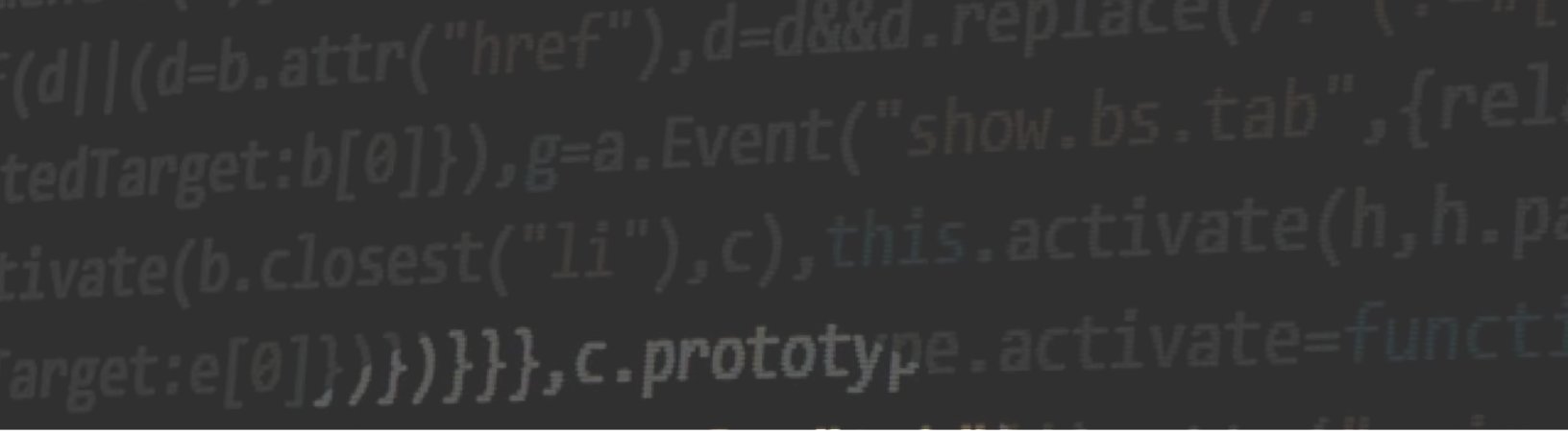
Further CISA research revealed that threat actors can bypass traditional trust models using Secure Sockets Layer (SSL) and other certificate authentications. Compromising open-source code is another popular vector used by threat actors; CISA found that malicious code is inserted into the public code libraries, such as C++ and Python, used by developers in building supply chain software. CISA's research also revealed that vendors' privileged access for many supply chain systems and applications are easily exploitable.

EXECUTIVE RESPONSE TO ESCALATING THREATS

The *America's Supply Chain* Executive Order, signed February 24, 2021, by President Biden, states that for the United States to establish economic prosperity and national security, a resilient, diverse and secure supply chain must be achieved.[i] The order brought to the fore recent cyberattacks and issued a directive instructing government entities to conduct supply chain risk assessments across a number of departments, namely the Departments of Energy, Health & Human Services, Commerce, Agriculture and Defense.

On May 12, 2021, a second executive order, *Improving the Nation's Cybersecurity*,[ii] outlined 10 approaches to managing cybersecurity. Importantly, the order established guidelines and reporting on the removal of barriers to facilitate the sharing of threat information and improve the detection of cybersecurity vulnerabilities. Section 4 details actions to enhance the security of the software supply chain:

> *The security of software used by the Federal Government is vital to the Federal Government's ability to perform its critical functions. 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. There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended. The security and integrity of "critical software"— software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources)—is a particular concern.*



Actionable requirements for government entities and, by association, government contractors include:

- Identify current tools, standards and best practices to assess software security
- Establish standards that can evaluate the security practices of the developers and the practice of suppliers
- Produce guidelines for secure software development environments such as administratively separate build environments, multifactor, risk-based authentication and conditional access across the organization, monitoring supply chain operations and responding promptly to attempted and actual cyber incidents

Implementation Concerns

The May 12, 2021, executive order highlights the sharing of information related to threats, specific vulnerabilities, and any associated incidents. The ability to share this information in a timely manner is essential for the preparedness and prevention of incidents from similar sources.

However, the reporting of activities and the liabilities related to cyber events, third parties and incidents have reputational and liability implications for private companies. Other examples of unintended implementation consequences include:

- Providing a Software Bill of Materials (SBOM) for each product or publishing code specifics to a public website
    - Bad actors and even unorganized attackers automate spider technologies to identify and attack standardized capabilities among private and government organizations.
- Publishing of a definition for the term “critical software” and then listing the categories of software and software products that fit the definition of critical software
    - Aggregation of leading software and software tools might allow attackers to join forces and target listed products and services in a prioritized fashion, making even more government and contractors vulnerable to threats

Spider technologies include web crawlers and spiderbots that systematically crawl the Internet creating web indexing often for future malicious use or exploitation.

The May 12, 2021, executive order also brings to light areas that require guidance and benchmarking. First the methodology must be established and then evolve more quickly than most government sharing can provide. Some best practice methodologies already are moving toward maturity as noted by the Defense Department's Security Requirements Guide Version 3.0 and the Federal Risk and Authorization Management Program (FedRAMP) Cloud Inspection Testing Program; however, organizations need more encouragement to take on a change management approach that emphasizes innovation. One workable suggestion may be a "Stop the Hacker" reporting utility offering quarterly recognition/rewards for the prevention of unique hacks, ransomware or other exploits so that early adopters of new technologies and practices encourage second- and third-wave adopters. Reducing liability for private companies that report real and potential threats could reduce hesitancy to contribute to more effective benchmarking, even with reporting being a requirement.

EMERGENT SCC FRAMEWORKS

NIST SP 800-53: Supply Chain Controls

In 2020, NIST updated Special Publication (SP) 800-53 to revision 5 and now features the SCRM Control family. SCRM controls are integrated throughout the other control families to help protect system components, services and products that form part of critical systems and infrastructures. The NIST SP 800-53 SCRM controls are a much-needed inclusion; they reflect industry guidance and acknowledge dependence on third-party vendors.

CMMC 2.0: Cyber Practices Certification

The Cybersecurity Maturity Matrix Certification (CMMC) version 2.0 was released in December 2021. CMMC 2.0 has been simplified to three levels. Accountability via annual self-inspections and senior leadership sign-off are new aspects of the certification program. Periodic external evaluations will use tangible artifacts or "proof-points," and they require organizations to understand the full scope of their supply chain in receiving information, data and connections to systems as they serve the DoD. CMMC will likely expand to other civilian agencies and their respective vendor chains in the near future. CMMC incorporates and is based upon NIST SP 800-171 and NIST SP 800-171A. Prudent small business would be wise to use an artifact-based self-assessment as they manage the annual sign-off requirement(s).

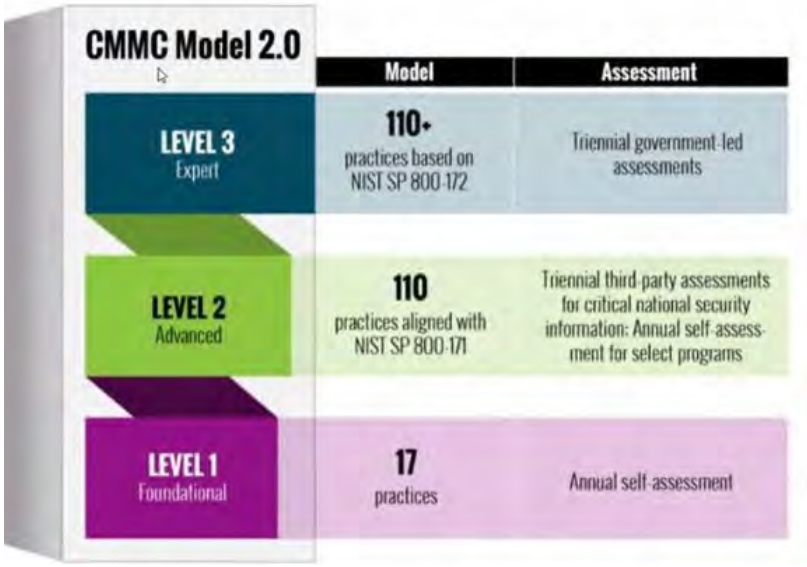
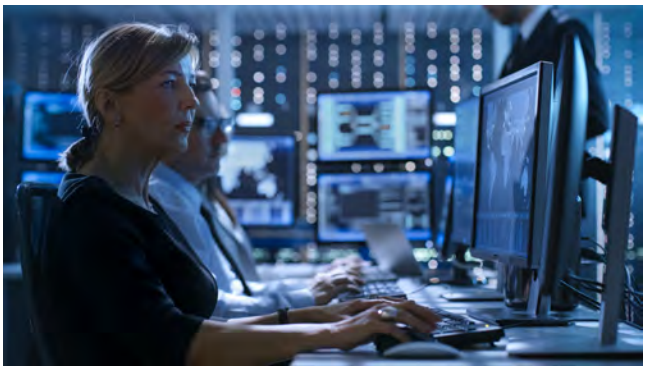


Figure-2: CMMC 2.0 Control Summary



NIST SP 800-171: Controlled Unclassified Information

The February 2020 revision of NIST SP 800-171 (current revision) *provides agencies with recommended security requirements for protecting the confidentiality of Controlled Unclassified Information (CUI) when the information is resident in nonfederal systems and organizations…The requirements apply to all components of nonfederal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components. The security requirements are* ***intended for use by federal agencies in contractual vehicles or other agreements*** *established between those agencies and nonfederal organizations.*[iii]

Federal Vendor Liabilities

An interesting consideration is the October 26, 2021, Department of Justice (DOJ) Civil Cyber- Fraud Initiative announcement regarding the use of the False Claims Act for federal contractors.

> *The initiative will hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches*[iv]*.*

Considering the DOJ and CMMC 2.0 announcements were released within 60 days of each other, and CMMC 2.0 requires annual senior management certification, it is likely that federal contractors (primes) will soon need to address CMMC 2.0 requirements that are based on the current revisions of both NIST SP 800-171 and NIST SP 800-53. We anticipate these requirements will cascade to subcontractors and their respective supply chains pursuant to the *Emergent Cybersecurity Frameworks and Executive Response to Escalating Threats* sections above.

BEST PRACTICE RESOURCES

To successfully address evolving cyber supply chain risks, organizations must engage internal operations processes and external capabilities for enterprise collaboration. Organizations need to strengthen strategies, procedures and experience levels in managing the supply chain from a cybersecurity perspective. A contractual and service level agreement (SLA) perspective can help baseline expectations for a more mature supply chain risk management/governance program.

CISA SCRM Toolkit

CISA, with representatives from private sector companies and associations, formed the ICT Supply Chain Risk Management task force to address threats faced by industry. One result of this working group was the *ICT Supply Chain Risk Management Toolkit.*

The task force webpage and subsection Resources to Strengthen Supply Chain Resilience can help enterprises navigate the vast amount of information available:

- Vendor SCRM Template provides scenarios and questions for ICT suppliers and vendors. The template provides clarity for strategic implementation, reporting and vendor vetting. Vendor SCRM Template also acts as a guide for supply chain risk planning in a standardized format. Sample *Vendor SCRM Template*

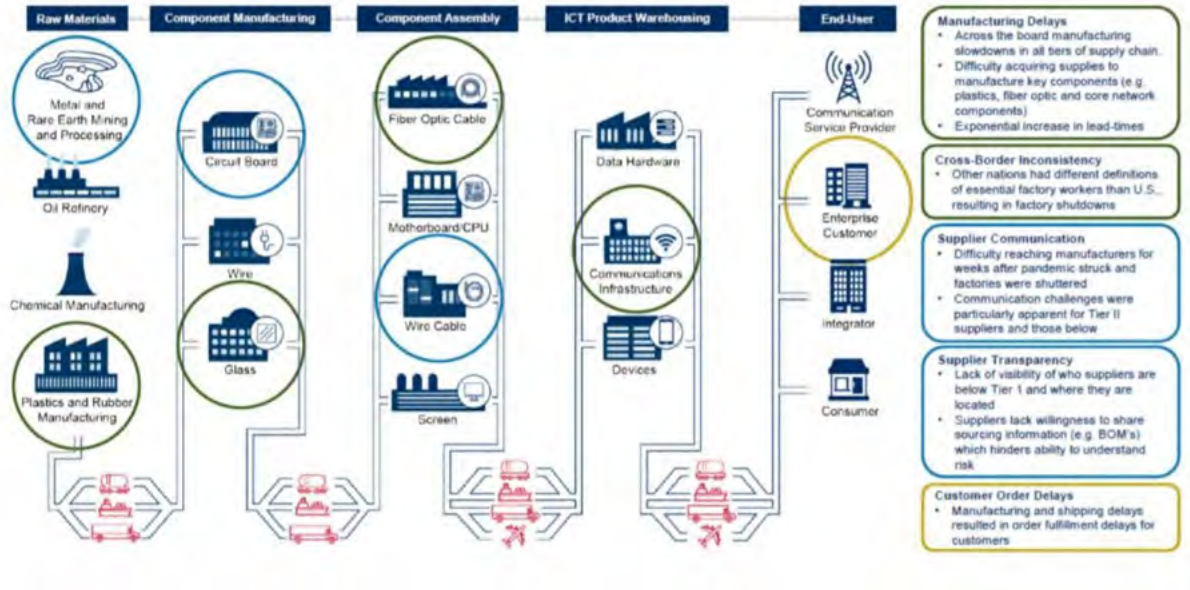
questions are provided in relation to supply chain implementation and are provided in Appendix A.

- *Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists* provides a list of components and standards that can be used to advise a company's decision on whether to build their own, seek alternative sources or rely on a qualified list for the acquisition of ICT products and services.

Both ICT tools are great starting resources for personnel with responsibilities along the cyber supply chain life cycle, particularly those with responsibility for development, distribution, deployment, acquisition or maintenance as well as procurement personnel who manage vendor and supplier lists.

The initial development of SCRM scenarios, vendor questions and mapping of information and material flows can be a daunting task for organizations of every size. One way to manage complexity is to develop a visual overview of the supply chain. The ICT task force's flow chart (below) provides an example of high-level systemic interdependencies from raw materials to transportation to end-user products. Strategic risks are grouped in color-coded boxes to the right, and colored circles relate these risks back to the supply chain sources.

APPENDIX A: ICT SUPPLY CHAIN SYSTEM MAP - PRODUCTION CHOKEPOINTS DURING PANDEMIC



Compliance Automation and NIST SP 800-53

Open Security Control Assessment Language (OSCAL) is a standard currently in development under the NIST banner. It is considered the 'standard of standards' because it provides a normalized expression of security requirements across multiple standards. Another important capability is the reason it finds itself in the resources section of this paper. OSCAL is a machine-readable representation of security information—from controls to system implementation to security assessment. In essence, OSCAL facilitates tool creation that bridges the gap between archaic approaches to IT compliance and innovative technology solutions.

OSCAL's link to the cyber supply chain is NIST 800-53 revision 5. This publication defines several cyber supply chain controls within the catalog of information security controls. The union was forged when the developers implemented multiple compliance and risk management frameworks (i.e., SP 800-53, ISO/IEC 27001&2, and COBIT 5) as part of OSCAL's pilot program. We continue to closely monitor OSCAL development and future deployment opportunities.

INITIAL STEPS TOWARD A HEALTHY CYBER SUPPLY CHAIN

Supply chain cybersecurity challenges are complex sets of issues that require a focused cybersecurity mindset based on context when determining which products and services are best suited for the organization. There is no single solution to solve all supply chain cyber problems.

The initial steps towards a healthy supply chain require executives, engineering, procurement, legal and compliance altogether to understand potential areas of cybersecurity weakness within the context of your organization:

- Identify where critical information is created, stored, transmitted and embedded in products and services all along your supply chain
    - Consider relevant aspects of *Emergent Cybersecurity Frameworks* above
- Develop scenarios and templates to baseline and prioritize your risks
    - Begin with internal operations scenarios
    - Develop a supply chain overview map showing interdependencies and strategic risks
    - Extend high priority scenarios to appropriate levels of your supply chain
- Examine contracts, service level agreements and policies for areas of potential liability
- Use vetted technologies to reduce immediate risks
    - Multifactor Authentication
    - Network segmentation including zero-trust practices
    - Leverage FedRAMP certified solutions
    - Encrypt data at rest and in transit
- Provide governance to any third-party solution or provider acknowledging shared risks
    - Once established, monitor vendor performance and any supplier risk changes
- Build out a permanent, workable SCC plan and capability

CONCLUSION

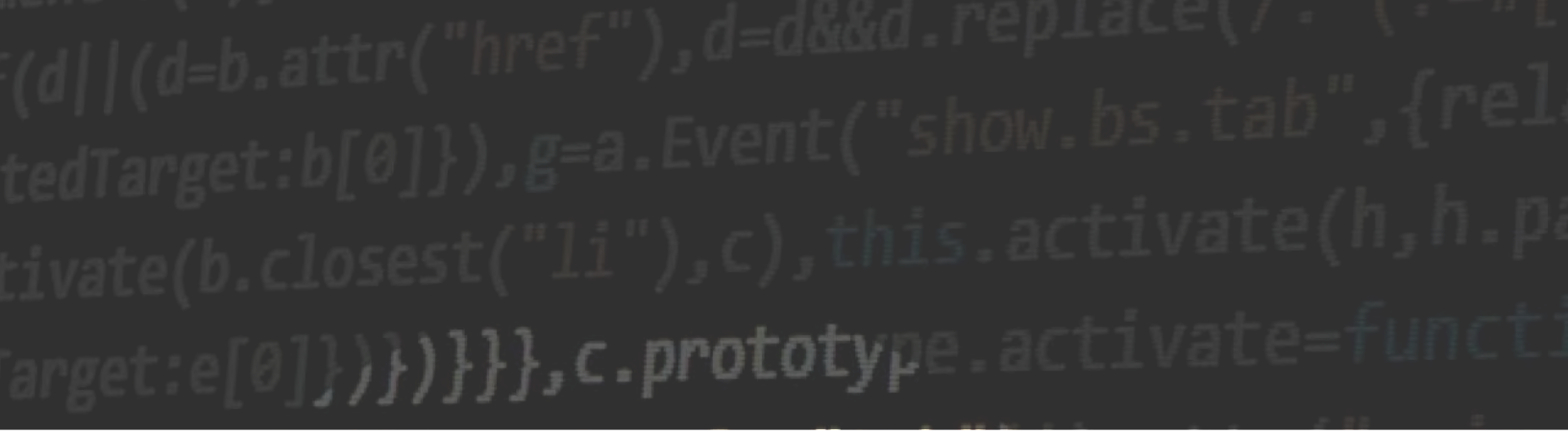
Supply chain cybersecurity management is the process of safely linking services and resources among entities. While it is reassuring to use existing skills and preferred management procedures, the reality is that new thinking is required to adapt to threats that are known—but invisible—to the daily operations of an organization. Contractual changes by the federal government enforcing accountability via civil and criminal liabilities will soon force organizations to prioritize and adapt internal processes and external supply chain relationships to prevent penalties.

Organizations such as CISA, NIST, International Organization for Standardization/International Electrotechnical Commission and industry-specific associations provide resources in the form of guidelines, standards and tools to help companies navigate this evolving risk environment.

Start now to review your supply chain risk management with fresh eyes! Your organization and clients need everyone to step up to the evolving challenges of supply chain cybersecurity in today's digital reality.

APPENDIX A: SAMPLE CISA *VENDOR SCRM TEMPLATE* QUESTIONS

Personal Security Questions	6.1—Does a formal personnel security program exist?
	6.6—Do you have a process for offboarding personnel?
	6.7—Are personnel security practices formally documented and accessible to employees?
	6.8—Are personnel security practices routinely enforced, audited and updated?
	6.9—Are personnel required to complete formal SCRM training annually?
	6.10—Are personnel trained in security best practices? This includes, but is not limited to, threats, access control and data protection?
	6.11—Is there additional security training provided to users with elevated privileges?
	6.12—Are you aware of security training practices performed by your sub-suppliers?
Supply Chain Integrity	7.1—Do your processes for product integrity conform to any of the following standards (e.g., ISO 27036, SAE AS6171, etc.)?
	7.2—Do you control the integrity of your hardware/software (HW/SW) development practices by using Secure Development Lifecycle Practices?
	7.4—Do you have processes in place to independently detect anomalous behavior and defects?
	7.6—Does the functional integrity of your product or services rely on cloud services?
	7.8—Do you have processes to evaluate prospective 3rd party suppliers' product integrity?
	7.9—Do you have regularly scheduled audits to ensure compliance with HW/SW products or services integrity requirements?



Supply Chain Resilience	8.1—Does your organization have a formal process for ensuring supply chain resilience as part of your product offering SCRM practices?
	8.2—Do you consider non-technical supply chain resilience threats such as weather, geo-political instability, epidemic outbreak, volcanic, earthquakes, etc.?
	8.3—Do you maintain a formal business continuity plan necessary to maintain operations through disruptions and significant loss of staff?
	8.4—Do you maintain a formally trained and dedicated crisis management team, including on-call staff, assigned to address catastrophic or systemic risks to your supply chain?
	8.6—Does your company consider supplier diversity to avoid single sources and to reduce the occurrence of suppliers being susceptible to the same threats to resilience?

APPENDIX B: PARTIAL LISTING OF STANDARDS, REGULATIONS, GUIDELINES FOR SCRM AND SUPPLY CHAIN CYBERSECURITY

1. Public Law 113 – 283; Federal Information Security Modernization Act of 2014
2. 252.204-7020 NIST SP 800-171 DoD Assessment Requirements; https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171-dod-assessment-requirements.
3. NIST Special Publication 800-171 Revision 2; Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations; https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
4. NIST Special Publication 800-171A final; Assessing Security Requirements for Controlled Unclassified Information; https://csrc.nist.gov/publications/detail/sp/800- 171a/final
5. NIST SP 800-53 Rev. 5; Security and Privacy Controls for Information Systems and Organizations; https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800- 53r5.pdf
6. Securing the Defense Industrial Base; CMMC 2.0; https://www.acq.osd.mil/cmmc/index.html
7. NIST's C-SCRM Program website: http://scrm.nist.gov
8. NIST's Case Studies and Key Practices in C-SCRM; Project: https://csrc.nist.gov/Projects/cyber-supply-chainrisk-management/key-practices
9. NIST's Supply Chain Interdependency Tool: https://csrc.nist.gov/Projects/cyber-supply- chain-riskmanagement/interdependency-tool
10. NIST-sponsored Research on C-SCRM: https://csrc.nist.gov/Projects/cyber-supply-chain- riskmanagement/NIST-Sponsored-Research
11. Software and Supply Chain Assurance Forum: https://csrc.nist.gov/Projects/cyber- supply-chain-riskmanagement/ssca
12. Federal C-SCRM Forum: https://csrc.nist.gov/federal-c-scrm

CONTRIBUTING AUTHORS

Maria C. Horton, CISSP-ISSMP, IAM

Maria Horton is a cybersecurity expert with experiences that span roles as a CEO/Founder of EmeSec Incorporated, a cloud security and engineering company, a FedRAMP Program Manager for DecisionPoint Corporation and a retired Navy commander who formerly served the National Naval Medical Center, now the Walter Reed Military Medical Center as chief information officer during 9/11. Horton holds the CISSP and ISSMP security credentials. Horton has published multiple times and has created two ebooks under the title banner #*SimplifyCUI*. The ebooks were recognized with two national awards in 2017. She presents regularly on risk management, IoT and cloud security. She is a member of the AFCEA Homeland Security Committee.

Shivaji Sengupta

Shivaji Sengupta is a management, solutions development and technology entrepreneur who has more than 27 years of experience providing solutions to government and commercial customers globally across 17 countries and four continents in the areas of cybersecurity, enterprise information management, content management and information technology. Sengupta 's companies NXTKey & Magnus provide information technology, information management, management consulting and cybersecurity solutions to federal and state government and commercial customers. Sengupta is an adjunct professor for cybersecurity at Delaware State University and an adjunct professor for computer science at Capitol Technology University. He is also a member of FBI InfraGard National Members Alliance (INMA), a board member for AFCEA International and an AFCEA Homeland Security Committee member.

---

i. Executive Order (E.O.) America's Supply Chain https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/.

ii. Executive Order on Improving the Nation's Cybersecurity, dated May 12, 2021; https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

iii. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

iv. https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative

The AFCEA International Homeland Security White Paper