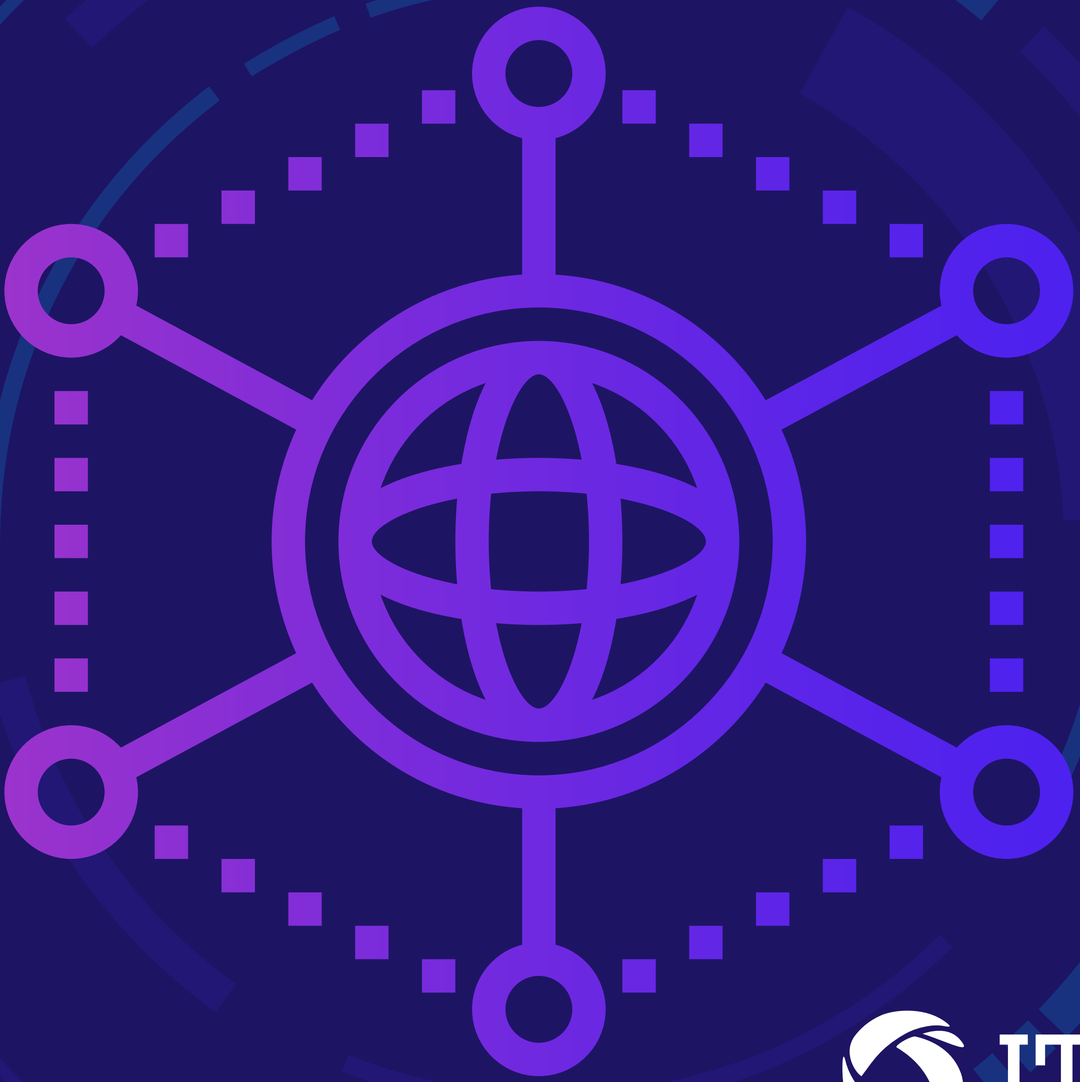
How the U.S. Government Can Secure its ICT Supply Chain: Recommendations for Public Sector Policymakers

March 2021



ITI
Promoting Innovation Worldwide

Executive Summary

Over the last few years, policymakers in the U.S. legislative and executive branches rightfully recognized that malicious actors could exploit the Federal information and communications technology (ICT) supply chain as an attack vector. However, the result has been a confusing patchwork of laws, regulations, executive orders and individual agency actions, many of which only consider a source's country of origin. To ensure the U.S. is well-positioned to proactively address supply chain risks holistically, ITI recommends that the current hodgepodge of policies be streamlined into a single, risk-based approach led by the Federal Acquisition Security Council (FASC). Policymakers should also reconsider what constitutes a "trusted supplier," optimize information sharing policies to incentivize industry participation, financially invest in supply chain risk management (SCRM), and hold individual agencies accountable for their SCRM posture.

Protecting Federal networks, data, infrastructure, and endpoint devices is one of the core responsibilities of the U.S. government. Failure to secure government and critical infrastructure systems can result in costly IP theft, exfiltration of private citizens' data, and an erosion of the U.S. national security posture. At the heart of this mission is the acquisition and deployment of modern, secure, and reliable information and communications technology (ICT). An increasingly globalized economy has led to a diversified marketplace, such that the design, manufacturing, and testing of critical ICT components occurs all around the world. While this global reality offers government agencies (and owners and operators of critical infrastructure) access to the most innovative and most cost-effective technologies, it also increases the complexity of monitoring for and protecting against supply chain threats. This could include tampering, the insertion of counterfeit parts into IT systems, malicious software, and insider threats.

The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, and related industries. Many of ITI's members are longstanding partners with the Federal government, providing innovative products and services intended to help government agencies execute on missions and power U.S. national security. ITI's membership has considerable first-hand knowledge of the challenging and evolving nature of cyber threats and wholeheartedly supports the important work of securing the Federal ICT supply chain.

Over the last few years, policymakers in the legislative and executive branches have recognized the importance of this issue and placed increased focus on protecting the Federal and critical infrastructure ICT supply chain. Despite the best of intentions, the sheer magnitude of the task of securing the supply chain has led to a sprawling and disjointed array of legislation, regulations, executive orders, and individual agency actions. Some of these efforts only consider Federal agency networks while others impose requirements on government contractors as well. Some are targeted merely at specific entities while others adopt a risk-based approach. A more complete inventory of U.S. supply chain policies can be found in Appendix A.

Nonetheless, the massive level of attention paid to Federal supply chain policy has not yielded effective government-wide supply chain risk management (SCRM) practices, but rather has added to the complexity and confusion of the cybersecurity requirements associated with IT acquisition. A recent report authored by the U.S. Government Accountability Office[1] found that agency adherence to seven National Institute of Standards and Technology (NIST) identified best practices to manage supply chain risks was lackluster at best. Of the 23 agencies surveyed, none had fully implemented all seven practices, and 14 agencies hadn't implemented any of the practices. Several agencies reported that they were waiting on government-wide guidance from the Federal Acquisition Security Council (FASC) before they were prepared to start implementing the practices.

The recent SolarWinds Orion breach, which was arguably the biggest supply chain cyber-attack in U.S. history, clearly demonstrates that a confusing web of inconsistent public policies with lackadaisical compliance and enforcement does little to protect Federal and critical infrastructure networks. Rather, that attack evinces a need for a thoughtful risk-based approach to SCRM policy. Heretofore, SCRM policy efforts have placed a myopic focus on a source's country of origin, or a blanket ban on certain named entities, failing to take into account the real risk of a foreign adversary breaching government networks by inserting malware through a U.S.-based company. **Recent events have taught us that we need a robust inter-agency Federal ICT supply chain risk management strategy that looks beyond a source's country of origin and fully considers the full range of threats, risk levels, and other appropriate mitigation steps.**

Thus, ITI recommends that the current patchwork of Federal ICT SCRM policy be streamlined into a single approach led by the FASC, with significant input provided by subject matter experts in the ICT industry[2]. A recent report on "Building a Trusted ICT Supply Chain" released by the *U.S. Cyberspace Solarium Commission*[3] echoes this suggestion, recommending government-wide supply chain strategies and programs to be "assessed and consolidated under a single vision." This approach would leverage existing Federal authorities and a coordinated inter-agency effort to drive near-term implementation of simplified, consolidated, and prioritized SCRM policies and practices. ITI also urges policymakers to reimagine our idea of a "trusted supplier" to consider proactive actions a vendor has taken to ensure compliance with SCRM best practices. Further, policymakers should create a supply chain risk information sharing policy that encourages industry participation, provide sufficient resources to ensure robust SCRM government-wide, and hold Federal agencies accountable for ensuring their own SCRM posture aligns with Federal standards.

A Note on Scope:

- Our recommendations concern ICT supply chain risk management as it relates to Federal networks and government procurement: We understand that other recent executive actions, most notably the *Executive Order on Securing the Information and Communications Technology Supply Chain*, concern whether U.S. companies can enter into transactions with certain sources in the commercial market, independent of whether the company has a business relationship with the Federal government. ITI plans to address this issue in additional policy guidance.
- Our recommendations do not address domestic sourcing or repatriationof supply chains for sensitive ICT components: ITI recognizes that U.S. reliance on foreign sources for crucial ICT components might create economic and national security risks in some cases. ITI strongly supports efforts to invest in domestic production of ICT components, such as the CHIPS for America provisions included in the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2021. We also believe the U.S. should develop a whole-of-nation and globally coordinated approach to ensuring U.S. leadership in key emerging and critical technologies and ready access to critical technologies from trustworthy suppliers. We do not address policy actions regarding sourcing and repatriation to address these risks in this paper but applaud the U.S. *Cyberspace Solarium Commission* for its efforts developing recommendations in this sphere.
- Our recommendations solely address cyber-supply chain risk management: NIST defines cyber-SCRM as the "process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of ICT/[Operational Technology] product and service supply chains." We will not address other supply chain risks to government contractors such as those posed by supplier use of human trafficking, child labor, and other nefarious labor practices or a reliance on conflict minerals.

Realign Government-wide Supply Chain Risk Management Policy Under the Federal Acquisition Security Council

The FASC was established in the 2018 SECURE Technology Act for the purpose of bringing supply chain and cybersecurity experts throughout the government together to address supply chain risks posed throughout the government acquisition process. The FASC is chaired by a designate from the U.S. Office of Management and Budget (OMB), and seven executive branch agencies are represented in its membership. The SECURE Technology Act also directs the FASC to work closely with industry in developing government-wide supply chain risk management guidance.

The FASC is granted an important authority to assess the supply chain risk posed by a source and, when necessary, issue a recommendation for excluding or removing the source from government networks. Upon receiving this recommendation, the Secretary of Homeland Security, the Secretary of Defense, and the Director of National Intelligence can issue an exclusion or removal order in their respective mission areas. If all three agency heads agree that a source poses an unacceptable level of risk, a government-wide exclusion or removal order will be carried out by the U.S. General Services Administration. Before issuing an exclusion or removal recommendation, the FASC must communicate the issue at hand to the source and give the source an opportunity to correct it. The SECURE Technology Act also requires the FASC to fully consider other mitigation options before issuing an exclusion or removal recommendation and provides impacted sources the opportunity to appeal a decision by the FASC and to seek judicial relief in the U.S. Court of Federal Claims.

Because of its inter-agency structure and its statutory directive to make risk-based decisions, ITI recommends that the SECURE Technology Act supersede any other identified SCRM policy that seeks to exclude or remove a source from government networks (including Sec. 889 of the FY19 NDAA, Sec. 1656 of the FY18 NDAA, and supply chain-related appropriations language from FY18 and FY20) and that the FASC be the sole entity responsible for maintaining a list of problematic or banned ICT equipment for the purpose of government procurement[4]. Though we acknowledge that the FASC is relatively new and many aspects of its operations are still unknown, we believe this is the best pre-existing entity to serve in this necessary central role. We recommend the following actions to strengthen the FASC and ensure it is best positioned to effectively conduct its mission:

1 The FASC must be granted a permanent collaborative mechanism for working with industry experts.

The Department of Homeland Security's (DHS) ICT Supply Chain Risk Management Task Force[5] has, over the last two years, brought together subject matter experts from industry and throughout the government (including many agencies that are represented on the FASC) to develop substantial SCRM-related best practices. This body should be considered the primary vehicle for the FASC's industry collaboration, and the FASC should lean heavily on the Task Force when developing its inter-agency guidance. We recommend that the Federal government permanently formalize this

Task Force, which was originally chartered on a temporary basis. This would enable the FASC to receive continuous feedback from industry that could inform updates to processes and improve the FASC's overall effectiveness. Working with industry is especially paramount when it comes to critical infrastructure partners, who play a leading role in Federal cybersecurity.

2 While modifications to legislation may be desirable in the mid-term to strengthen an enterprise-wide approach to Federal security, current authorities enable OMB, the FASC, NIST, and DHS to develop, oversee, and support implementation of security policies and to direct agency activities.

The Federal Chief Information Security Officer and the recently established National Cyber Director can facilitate more robust cross-government coordination and implementation of existing as well as in-development supply chain risk management best practices. In conjunction with the above agencies, the FASC should also consider how to integrate NIST SP 800-161, *Supply Chain Risk Management for Federal Information Systems* and the *Framework for Improving Critical Infrastructure Cybersecurity v1.1* (NIST Cybersecurity Framework). The FASC should also pursue consistency with ongoing processes to evolve global standards, including International Standards Organization (ISO) 27036[6] on Information Technology / Security Techniques (treatment of information risks involved in the acquisition of goods and services), SAE/G32 on Cyber Physical Systems Security[7] and others supporting interoperability security across Federal and global environments.

3 The FASC must ensure that its guidance lays out a fair process for issuing exclusion and removal recommendations that is shielded from potential abuse by a source's competitors.

To address principles of both due process and fairness, the FASC should consider requiring any information submitted to be corroborated by multiple sources prior to initiating an investigation based on that information. To ensure the integrity of Federal supply chain risk management processes, the Federal government should work closely with the FASC to establish remedies or safeguards in the event of false claims against a company, using the suspension and debarment procedures outlined in the Federal Acquisition Regulation (FAR) Subpart 9.4 as a model.

4 The FASC should work closely with the U.S. Treasury Department's Committee on Foreign Investment in the United States (CFIUS) to develop risk criteria relating to foreign control or ownership of a source.

The FASC should *not* consider a source to pose a risk solely because the source conducts operations overseas, as this would be so broad as to apply to every major U.S. company regardless of any actual risks present. The risks presented by a particular U.S./foreign business relationship must be analyzed based on the specific facts and circumstances, with strong consideration of any risk mitigation options already in place (for instance, if the source has signed a CFIUS National Security Agreement). Further, the need to address underlying security concerns must balance with American business' global competitiveness, which often depends upon relationships with foreign entities, and ability to innovate. In other words, foreign control or ownership can be considered a risk factor, but not the only factor as to whether the source poses a risk to Federal networks, particularly as it relates to U.S. allies. For example, an information processing or data storage component holding or transacting on sensitive data should be viewed differently than a simple and testable mechanical part that poses little risk even if it fails.

5 Every exclusion and removal recommendation issued by the FASC should be narrowly tailored to address an articulable security risk, tied to particular products that present the highest levels of risk, and time limited.

An entity subject to an exclusion or removal recommendation should have a clear process for submitting evidence that can trigger a reassessment. These decisions should consider the capability to cause harm to our national security and not just whether harm has occurred in the past.

6 In its guidance, the FASC should clearly detail what is expected of all Federal contractors (including prime and subordinate contractors) in the process of removing banned IT equipment from Federal networks.

This includes guidance on the extent to which contractors must make efforts to determine if banned equipment is found within their existing systems. We recommend that the FASC consider using the same standard employed in FAR Case 2019-009, *Prohibition on Contracting with Entities Using Certain Telecommunications or Video Surveillance Equipment or Services*, which requires contractors to conduct a "reasonable inquiry" of information in the entity's possession as to whether they use the impacted equipment. The extent to which the equipment is used by the contractor should also be taken into account (for instance, if the equipment is used exclusively in a closed network or its use is air-gapped from the company's U.S. operations).

Moreover, use of any banned equipment that that does not touch the Federal supply chain should not in any way impede a company from working with the Federal government. For instance, in many overseas jurisdictions, the only way to connect to a network is to use equipment that has already been banned in previous rulemaking. A blanket ban of contractor use of such equipment would be impracticable for all companies with overseas operations and will severely limit the Federal government's ability to procure the latest and most innovative technologies.

7 The FASC should coordinate the administration and execution of existing authorities to strengthen supply chain risk management.

Better utilization of existing authorities could rapidly improve supply chain security. For example, the FASC could: Publicize its recommendations for any legislative, regulatory, or other policy changes to incentivize industry adoption of best practices for supply chain risk management, as required in the SECURE Technology Act; identify criteria that would automatically require FASC reviews under the SECURE Technology Act; and finalize the requirement under the FY2019 NDAA for DoD vendors to disclose whether source code has been shared with countries of concern.

8 In developing its SCRM guidance for government agencies, the FASC should develop a risk-based frameworkthat establishes which types of procurements or missions necessitate a higher level of assurance.

ITI recommends that the FASC look to the recently released *DoD Instruction 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers*[8] as a guide. In addition, the FASC should look at how related guidance from the Committee on National Security Systems[9] and the Intelligence Community[10] can be integrated with the DoD Instruction's model. In particular, the DoD issuance creates a framework for cyber-SCRM due diligence that links supply chain risk tolerance with the level of mission criticality of the systems purchased:

SCRM Considerations in *DoD Instruction 500.90*

- **High Risk Tolerance (for simplified procurements):**

  Program Managers (PMs) should exercise caution against procuring items with a foreign source and leverage approved products lists and industry standards. ITI believes these foreign source decisions should consider whether the country has a stated or implied objective to cause harm or damage to U.S. national interest.

- **Moderate Risk Tolerance (for structured procurements such as wireless networks at a forward deployed base):**

  PMs should implement all previous strategies and use verifiable vendor processes for product integrity as well as manage critical SCRM risks through countermeasures.

- **Low Risk Tolerance (for engineered procurements like industrial controlled systems):**

  PMs should implement all previous strategies and assess critical components, integrate available countermeasures, and leverage commercial assessment vendors as well as trusted international partners and national labs.

- **Very Low Risk Tolerance (for assured procurements like nuclear command and control systems):**

  PMs should implement all previous strategies and follow the NIST SP 800-161 and DODI 5200.44 SCRM guidance.

Reimagine What It Means to Be a Trusted Supplier

Much of the discourse around supply chain risk management policy centers around what constitutes a "trusted supplier." The Prague Proposals[11] endorsed by the U.S. government at the Prague 5G Security Conference as well as recommendations released by the Center for Strategic and International Studies (CSIS)[12] fully consider what it means to be a trusted 5G vendor. Particularly, the CSIS recommendations acknowledge that while a source located in an adversarial nation state can pose a security risk, there are significant mitigation actions a source can take to offset that risk. ITI supports these recommendations and believes they can be extended beyond 5G network equipment to the broader IT ecosystem. However, to the extent that actual U.S. policies have attempted to define what "trustworthiness" means, the bulk of these actions have focused solely on a source's country of origin. Consequentially, this approach fails to account for the possibility of a U.S.-based company being compromised and used as a conduit for a foreign-based malware attack.

Especially when it comes to 5G cybersecurity, focusing on the trustworthiness of specific vendors is a too-narrow approach that does not enable effective management of all risks. State-of-the-art security tools and capabilities exist that operators can use to manage today's cybersecurity risks and secure their networks and data, regardless of the underlying technology or vendor.

The ICT SCRM Task Force's Working Group Two, which was tasked with cataloguing the universe of threats to the Federal supply chain, **found that a potential source's country of origin accounts for only one of 188 identified supplier-related threats**[13]. Policymakers must recognize that the U.S. operates in a global economy and many ICT products will be manufactured overseas. As long as the Federal government prioritizes commercially available off-the-shelf (COTS) items and values working with allies, Federal SCRM policy must factor this in. Without access to the global marketplace and global talent, high functioning, low-cost COTS products could not exist. Thus, our understanding of what aspects of a vendor's operations pose a risk and how these risks can be mitigated must evolve.

In order to proactively guard itself against future attacks, the U.S. government must expand its understanding of what constitutes a trusted supplier and provide vendors with an opportunity to prove their capabilities.

1 To reduce the risk of counterfeit parts being inserted into the ICT supply chain, the U.S. government must instruct its acquisition personnel to, when possible, prioritize and fast-track procurements for ICT equipment and services from original equipment manufacturers (OEMs) and their authorized distributors or resellers, except where an organization has a comprehensive supply chain security program sufficient to mitigate the counterfeit part's risk.

Any such instruction must include both Contracting Officers (COs) and Government Purchase Card holders, who typically do not receive training in the FAR. The draft FAR language written by the ICT SCRM Task Force Year One Working Group Four[14] should be used as a guide.

2 Agency personnel should leverage, where possible, Qualified Bidder Lists, Qualified Manufacturer Lists, and Approved Products Lists.

Programmatic staff should refer to recommendations issued by the ICT SCRM Task Force Working Group Three to determine when and how to construct a Qualified Bidder List, Qualified Manufacturer List, or Approved Products List. Agency staff should establish criteria for ensuring that these approved lists are kept contemporary.

3 Vendors and potential vendors should have the opportunity to proactively assert their maturity by demonstrating the actions they take to protect their networks and supply chains through enhanced cybersecurity program certifications and product security mechanisms.

Examples of program attestation could be a signed CFIUS National Security Agreement, Customs Trade Partnership Against Terrorism (CTPAT) certification, a certificate from the Cybersecurity Maturity Model Certification (CMMC) Accreditation Body, or demonstrated compliance with NIST SP 800-161 or other global, industry-led standards like International Standards Organization (ISO)/International Electrotechnical Commission (IEC) 20243[15] , ISO/IEC 27036, and the International Society of Automation (ISA)/ International Electrotechnical Commission (IEC) 62443 suite of standards for industrial automation systems cybersecurity[16]. Enhanced product security practices, such as Software Bill of Material (SBOMs), sophisticated cryptographic code-signing and use of the ICT SCRM Task Force Working Group Four Vendor SCRM Template, should be encouraged as a means for vendors to demonstrate a commitment to following SCRM best practices.

Contracting personnel should strongly consider these attestation mechanisms offered by potential vendors when evaluating bids and, in recognition of the considerable compliance investments government contractors have made to prove their cybersecurity capabilities, allow for reciprocity between schemes.

4 Policymakers should consider a model whereby the government publishes security requirements, and then asks vendors to self-attest to those requirements.

A great example of this model can be found in the UK's Cloud Security Principles[17]. Under this system, the UK government specifies the 14 principles that cloud service providers should abide by and implement in their offerings, while also providing a guide for government agencies/departments on how to make informed risk decisions while evaluating vendor claims. This does away with the need to create a cottage industry of third-party auditors/assessors, shortens timelines and reduces authorization costs by eliminating the need for a months-long audit process, and thus makes innovative products immediately available for government consumption. If the Federal government were to adopt such a model, policymakers should provide a pathway for reciprocity for existing compliance investments. This will limit the conversation to net new Federal requirements and may lead more quickly to a comprehensive unified industry standard for supplier compliance.

5 Consider SCRM maturity for sub-contractors.

For the broader ecosystem, Federal acquisition requirements will have cascading impacts on practices (given that Federal suppliers should be required to assess their own suppliers). The U.S. government should also consider creating a program through which organizations could promote their adherence to tiered requirements for supply chain and cyber risk management.

Invest in Federal ICT Supply Chain Risk Management

Because protecting Federal networks and infrastructure should be considered a fundamental government mission, policymakers must make considerable investments in the personnel, operations, and equipment that can best secure the ICT supply chain.

1 A FASC tasked with managing government-wide SCRM decision-making will require considerable resources in order to carry out this important work.

ITI recommends that Congress authorize a formal Program Management Office (PMO) under OMB for the FASC's operations. This PMO could be allocated resources through a shared services funding model, with contributions from the DoD and GSA budgets, among others. Without dedicated funding for the FASC's operations, the body will not be able to perform its statutory objectives.

2 Targeted investment in IT modernization, including cross-existing government programs, will be a crucial part of securing the Federal ICT supply chain.

Government agencies spend approximately 70 percent of IT dollars to operate and maintain legacy systems—a reliance on these types of systems creates considerable supply chain and cybersecurity risks, as contracting personnel are more likely to turn to the gray market to find necessary replacement components. Policy makers can accelerate the deployment of transformational IT modernization technologies and limit the use of "gray market" products by enabling greater cross-government efficiencies when assessing the security of IT products and services. A 2019 GAO report[18] found that nearly two thirds of surveyed agencies were realizing "significant" performance, security, and cost benefits, including a combined savings of $291 million through the increased use of cloud services through the existing Federal Risk and Authorization Management Program (FedRAMP).

The American Rescue Plan proposed by President Biden describes the need for emergency funding to upgrade Federal IT infrastructure and address recent cyber breaches as an "urgent national security issue that cannot wait." ITI supports the robust funding to modernize and secure Federal IT systems and networks as enacted in this legislation.

Furthermore, the SolarWinds incident revealed a lack of comprehensive, real-time visibility of the networks and Internet-facing assets that agencies are responsible for monitoring, protecting, and defending. A key lesson learned from the incident is the urgent need to focus cybersecurity funding on technologies beyond signature-based defenses, such as AI/Machine Learning (ML)-based user behavioral analytics at the end point, and technologies that effectively collect, integrate, and normalize security data across the entire network enterprise, automating defensive capabilities wherever possible to assist with incident response. This is especially true for agencies that have established centralized monitoring, like DHS's Continuous Diagnostics and Mitigation (CDM) program.

Hold Federal Agencies Accountable for Their SCRM Posture

The Government Accountability Office's finding that the Federal agencies surveyed in its report do not have proactive, comprehensive SCRM plans is concerning. While government-wide guidance from an inter-agency body coupled with robust Federal investment in SCRM will go a long way, ultimately agencies will bear responsibility for implementing this guidance and protecting the Federal ICT supply chain. Thus, ITI recommends that policymakers incentivize individual agencies to fully implement any identified best practices from the FASC and improve their SCRM posture.

1 Adherence to SCRM guidance released by the FASC should be imputed into the U.S. House Committee on Oversight and Reform's Federal Information Technology Acquisition Reform Act (FITARA) Scorecard.

This semi-annual scorecard gauges agencies' progress in improving their IT posture. Adding SCRM to the FITARA Scorecard will demonstrate that the U.S. government considers it equal in importance to other elements of Federal IT like agency CIO authority enhancements, updating legacy systems, and the Data Center Optimization Initiative.

2 Ensure consistency around designation of National Security Systems.

Any risk-based framework released by the FASC will impose stringent requirements on the most mission-critical systems and networks, such as National Security Systems (NSS). This might create a disincentive for personnel to correctly identify such a system as an NSS. Any agency performing classified work must create centralized guidance as to when a system should be designated as an NSS. This guidance must align with existing frameworks like NIST 800-161 where possible and agency compliance with this guidance must be assessed during annual FISMA audits.

3 IT spend, including Technology Modernization Fund (TMF) dollars, should be tied to an agency's SCRM performance and compliance with guidance released by the FASC.

TMF funding currently includes a five-year payback requirement for agencies that take advantage of the program, and this creates a strong disincentive for agencies to take concrete, permanent action to modernize their IT systems. ITI proposes that the TMF payback requirement be partially waived for agencies that can prove full compliance with any SCRM guidance released by the FASC and fully waived for full compliance with all identified Federal cybersecurity requirements.

Optimize Information Sharing Processes

ITI recognizes that the SECURE Technology Act tasks the FASC with establishing an information sharing process with the ICT industry. Bi-directional information sharing between the Federal government and private sector partners can help both parties more easily identify and mitigate supply chain risks. The type of risks typically shared can include product-based risks (such as counterfeit products or the insertion of malware) and organizational risks (such as insider threat behavior). The ICT SCRM Task Force's Working Group One found that many types of risk information are available, but the sources were little known, not affordable, or not easily accessible[19]. Moreover, there are considerable hurdles preventing industry from freely sharing and receiving risk information that must be changed to facilitate effective communication and collaboration.

1 Remove legal barriers to risk information sharing.

Vendors face enormous legal risks when revealing supplier-specific information that might be derogatory. Though the Cybersecurity Information Sharing Act and the Critical Infrastructure Information Act offer some legal protections, many contractors note that the potential cost of litigation makes information sharing and participating in groups like Information Sharing and Analysis Centers (ISACs) prohibitively expensive. ITI suggests that policymakers develop robust liability protections for vendors that share risk information in good faith.

2 Expand audience for government risk information sharing.

ITI members have reported that detailed risk information shared with industry from the government is typically dispersed only to individuals that hold security clearances. In many cases, officials aren't willing to share this information with industry even if they have appropriate clearances. This is problematic because high-level decisionmakers that can have the most impact on an organization's SCRM practices are not likely to hold a clearance. The Federal government should look for a way to communicate risk information in an unclassified but timely and safe manner.

3 Create reasonable transparency around the Vulnerabilities Equities Process (VEP).

Oftentimes, Federal personnel will decide to withhold certain risk information (for instance, a vulnerability found in a vendor's product) so that the information can be used for other purposes. VEP is used by Federal officials to determine whether they should disclose zero-day security vulnerabilities. We recommend that this Process include a consideration of the necessary balance for cybersecurity offensive and defensive capabilities, and be as transparent with industry as possible in government use of discovered vulnerability information, potentially with an annual classified report.

4 The U.S. government should strengthen cybersecurity information sharing with key allies, particularly those countries who share a robust defense and trade relationship with the United States to ensure that any cyber-vulnerabilities identified by allies are shared with the U.S. government.

Such relationships create a multiplying effect, expanding the ability of the U.S. government to monitor and identify cyber-vulnerabilities.

Conclusion

The risks posed to the Federal ICT supply chain are varied and complex, and constantly evolving. Mitigating these risks will require a significant investment of time, resources, and collaboration among key actors across government and industry.

ITI believes that a coherent, streamlined approach, as articulated in this document, can substantially advance the goal of securing government and critical infrastructure systems. This approach which unifies Federal ICT supply chain efforts under a single, coordinating authority (the FASC), articulates clear and transparent security standards for industry vendors and service providers, prioritizes long-term Federal investment in SCRM, holds Federal agencies accountable for their SCRM posture and optimizes information sharing processes, presents a logical, achievable roadmap for success in addressing this critical national security issue.

References

[1] https://www.gao.gov/products/GAO-21-171
[2] A Note on Scope
[3] https://www.solarium.gov/public-communications/supply-chain-white-paper
[4] The SECURE Technology Act grants individual agency heads a separate authority to exclude and remove problematic IT equipment from their own agency's networks. ITI believes agency heads should retain this authority, especially while the FASC is still working to develop its own guidance but urges agency heads to confer with the FASC and other inter-agency bodies when considering whether to ban a source from its networks.
[5] https://www.cisa.gov/ict-scrm-task-force
[6] For more information, see https://www.iso27001security.com/html/27036.html
[7] For more information, see https://www.sae.org/works/committeeHome.do?comtID=TEAG32
[8] https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500090p.PDF?ver=MIG3uLnzXl31QcvXJTZ5uA%3D%3D
[9] https://www.cnss.gov/CNSS/openDoc.cfm?pj8ZmiWC4KgKxB1UgLOAxA==
[10] https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats
[11] https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/
[12] https://www.csis.org/analysis/criteria-security-and-trust-telecommunications-networks-and-services
[13] https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report_0.pdf
[14] https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management% 20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf
[15] For more information, see https://www.iso.org/standard/74399.html
[16] For more information, see https://www.iso.org/standard/74399.html
[17] Available at https://www.ncsc.gov.uk/collection/cloud-security.
[18] https://www.gao.gov/assets/700/698236.pdf
[19] https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf

Appendix

Inventory of Federal Supply Chain Risk Management Programs

1. Compiled by the Information and Communications Technology (ICT) Supply Chain Risk Management Task Force Coordination Tiger Team
2. Department of Homeland Security Cybersecurity and Infrastructure Security Agency ICT Supply Chain Risk Management (SCRM) Task Force
3. Outsourcing of Network Services Assessment Tool (ONSAT) Tool (formerly "Risk Management of Outsourced Network Services (RMONS)" – Out of the Enduring Security Framework (ESF)
4. Federal Acquisition Security Council (FASC)
5. Department of Commerce Bureau of Industry and Security (BIS) – Entities List
6. Bureau of Industry and Security (BIS) — De Minimus Regulation
7. Bureau of Industry and Security (BIS) – Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List
8. National Telecommunications and Information Administration (NTIA) Software Bill of Materials (SBOM)
9. National Institute of Standards and Technology (NIST) Internal Report (IR) 8276 - Key Practices in Cyber Supply Chain Risk Management: Observations from Industry
10. NIST IR 8286: Integrating Cybersecurity and Enterprise Risk Management
11. NIST Special Publication (SP) 800-161 Rev. 1 - PRE-DRAFT Call for Comments: Supply Chain Risk Management Practices for Federal Information Systems and Organizations
12. NIST Special Publication (SP) 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
13. NIST National Cybersecurity Center of Excellence (NCCoE) – Supply Chain Assurance Project
14. Executive Order (EO) 13873 Securing the Information and Communications Technology and Services Supply Chain
15. Protecting Against National Security Threats to the Communications Supply Chain Through FCC [Federal Communications Commission] Programs (FCC 19-121)
16. Supply Chain Notice of Proposed Rulemaking (NPRM)
17. Final Designation Proceeding for Huawei Technology Company
18. Final Designation Proceeding for ZTE Corporation
19. Communications Security, Reliability, and Interoperability Council (CSRIC)
20. Executive Order on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector
21. Department of Defense Cybersecurity Maturity Model Certification (CMMC)
22. National Defense Authorization Act (NDAA) Section 889 Federal Acquisition Regulation (FAR) Rule Implementation
23. Alliance for Telecommunications Industry Solutions (ATIS)/DOD 5G SCRM
24. Department of Energy SCRM Plan
25. Executive Order 13920: Securing the United States Bulk-Power System
26. Telecommunications Industry Association (TIA) SCRM Efforts
27. Cyberspace Solarium Commission
28. New Committee on Foreign Investment in the United States (CFIUS) Legislation
29. National Strategy to Secure 5G of the United States
30. Public Law 116-124: Secure and Trusted Communications Networks Act of 2019
31. Public Law 116-129: Secure 5G and Beyond Act of 2020
32. Utilizing Strategic Allied (USA) Telecommunications Act (Introduced in Senate)

ITI

Promoting Innovation Worldwide

www.itic.org