Securing Critical Supply Chains: Strategic Opportunities for the Cyber Product International Certification (CPIC™) Initiative

Paul Stockton

China, Russia, and other potential adversaries are increasing their efforts to corrupt the supply chains upon which the electric grid and other infrastructure sectors depend. Valuable initiatives are underway to strengthen supply chain risk management (SCRM). Yet, despite these measures, the US intelligence community warns that the growing scale and sophistication of attacks on the supply chain "are placing entire segments of our government and economy at risk."[1] Similar challenges confront Israel, the United Kingdom, and other US security partners.

At present, infrastructure owners and operators lack a compressive, stakeholder-driven process to certify that crucial hardware and software products are even minimally scrubbed of malware and other means of adversary exploitation. Establishing such a certification process contribute enormously to cyber resilience,

Dr. Paul Stockton is the managing director of Sonecon, LLC, and a former US assistant secretary of defense for Homeland Defense and America's Security Affairs. Robert Denaburg, a senior analyst at Sonecon, performed research for the report. The findings and recommendations in this article are solely those of the author and do not necessarily reflect the views of the Department of Defense or any other US government agency.

1 National Counterintelligence and Security Center, "Supply Chain Risk Management: Intelligence.Gov Background Paper," March 2017, p. 2, https://www.dni.gov/files/NCSC/documents/products/20170317-NCSC--SCRM-Background.pdf.

especially if government agencies can provide threat information and other forms of support for the initiative.

The Cyber Product International Certification (CPIC) initiative proposed by the Electric Infrastructure Security (EIS) Council will help meet these challenges. CPIC could add even greater value for infrastructure resilience by including measures to certify products against intentional electromagnetic interference (IEMI).

Keywords: Cyber, threats, supply chain, OT, energy, CPIC

The Scope and Severity of the Threat

The risks posed by Russian and Chinese hardware and software to infrastructure resilience (and to national security) have garnered intense government scrutiny in recent months.[2] However, products sold by ZTE, Huawei, and Kaspersky Labs constitute only the publicly visible "tip of the iceberg" of hostile efforts to corrupt supply chains and enable potential adversaries to establish persistent presence in US and partner networks.

In the Department of Homeland Security's May 2018 "Cybersecurity Policy," the department warns that the growing connectivity of modern infrastructure sectors and services introduces new vulnerabilities and "opens the door to potentially catastrophic consequences from cyber incidents."[3] This is attributed in part to a reliance on increasingly global supply chains and the rapidly expanding number of internet-connected devices, which—without countervailing innovations that emphasize improved security and resilience—will continue to intensify supply chain risk management (SCRM) challenges.[4] Despite the current array of public and private sector programs to mitigate and counter supply chain threats, "the evolution of

2 See, for example, Danny Lam and David Jimenez, "US' IT supply chain vulnerable to Chinese, Russian threats," *The Hill*, July 9, 2017, http://thehill.com/blogs/pundits-blog/technology/341177-us-it-supply-chain-vulnerable-to-chinese-russian-threats; Joseph Marks, "Chinese Telecoms Could Join Kaspersky On Government wide Banned List," *Nextgov*, February 13, 2018, http://www.nextgov.com/cybersecurity/2018/02/chinese-telecoms-could-join-kaspersky-governmentwide-banned-list/145960.

3 Department of Homeland Security, "Cybersecurity Strategy," May 15, 2018, p. 1, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

4 Ibid., pp. 22–23.

directed, sophisticated and multifaceted threats threatens to outpace our countermeasures."[5] Given the current threat environment and global supply chain trends, "cyber SCRM is not optional."[6]

While adversaries cannot remotely insert and exploit electromagnetic vulnerabilities in the same way they can with cyber weapons, a number of risks also exist. For example, adversaries could introduce components that are faulty or particularly susceptible to electromagnetic threats into infrastructure supply chains. Adversaries could also attempt to capitalize on known electromagnetic vulnerabilities in widely-deployed components, augmenting the potential damage caused by an electromagnetic attack.

Threats to global supply chains are multifaceted, and several factors and trends are intensifying these threats. This intensification of supply chain threats pose a number of challenges for successfully mitigating them as well as an imperative to do so.

1. Increasing number of threat vectors

Adversaries continue to find innovative ways to target, corrupt, and exploit supply chains. Indeed, the increasing global complexity of supply chains and intensification of adversarial threats have amplified the risk that suppliers could intentionally or unintentionally introduce compromised hardware, software, or firmware into a system or network.[7] New information technology (IT) initiatives such as cloud computing and the Internet of Things (IoT) have also expanded the cyber supply chain attack surface,[8] increasing the number of possible infiltration points that adversaries can target and creating additional challenges for infrastructure owners and operators in securing their supply chains.

Adversaries are seeking opportunities to corrupt every point in the global supply chains that support US infrastructure. Risks exist at each stage: design,

5 "Supply Chain Risk Management: Intelligence.Gov Background Paper," p. 2.

6 National Institute of Standards and Technology, "Best Practices in Cyber Supply Chain Risk Management," n.d., p. 1, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Business-Case.pdf.

7 Ibid., p. 1.

8 Jon Oltsik, "Protecting the Cyber Supply Chain," *Cipher Brief*, December 6, 2015, https://www.thecipherbrief.com/article/protecting-cyber-supply-chain.

manufacturing, integration, deployment, and maintenance.[9] Adversaries may insert vulnerabilities into the supply chain themselves, or can potentially capitalize on latent, inherent vulnerabilities yet to be addressed by security practitioners.[10]

Even if a vulnerability does not exist in the initial development, adversaries can insert them at any point in the life cycle of a system.[11] This includes software updates or vulnerability-correcting "patches" for IT or operational technology (OT) systems which can upload malicious code into a system, or insert malignant firmware for exploitation at a later date.[12] The frequency with which system operators apply software updates creates multiple opportunities for adversaries to compromise systems long after the design stage.

Adversaries may also compromise the hardware that utilities install in their operating systems. For example, a Defense Science Board (DSB) report noted numerous potential vulnerabilities associated with supply chain compromise of microelectronics. While the DSB report focuses on weapons systems, similar microelectronics are increasingly present in every infrastructure sector. These microelectronics "will inevitably contain latent vulnerabilities" that may be discovered only years after the product enters into service—if at all—and potential effects range from system degradation to system failure.[13]

Software updates are especially prone to hostile efforts to gain persistent access to counter-intelligence networks, which adversaries could later use to launch disruptive attacks on infrastructure operations. For example, the Russian Dragonfly campaign initially targeted "peripheral organizations such

9 National Counterintelligence and Security Center, "Supply Chain Risk Management: A Framework for Assessing Risk," February 2013, p. 2, https://www.dni.gov/files/NCSC/documents/products/SCRM_Framework_for_Assessing_Risk_White_Paper.pdf.

10 Public-Private Analytic Exchange Program, "Identifying and Mitigating Supply Chain Risks in the Electricity Infrastructure's Production and Distribution Networks," 2016, p. 4, https://www.dni.gov/files/PE/Documents/Electricity-Infrastructure-Summary.pdf.

11 Defense Science Board, "Task Force on Cyber Supply Chain," February 2017, p. 1, https://www.acq.osd.mil/dsb/reports/2010s/1028953.pdf.

12 The Public-Private Analytic Exchange Program, "Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions," 2017, p. 12.

13 Defense Science Board, "Task Force on Cyber Supply Chain," February 2017, pp. 1–2.

as third-party suppliers with less secure networks," using them as staging targets to pivot to intended victims.[14] ICS cybersecurity firm Dragos, Inc. also recently profiled a threat actor that has targeted ICS networks, through the use of watering hole attacks to steal credentials and gain access to compromised victims' networks and machines.[15]

2. Covert ownership and globalization of supply chain vendors

Supply chains are becoming increasingly global. As supply chains become ever more intricate and international, the most capable adversaries "can access this supply chain at multiple points, establishing advanced, persistent, and multifaceted subversion."[16]

Ownership, control, and/or influence of points along global supply chains by malicious governments or government-affiliated corporations are particularly concerning. Software and firmware code is developed by suppliers in many countries, which "opens up plenty of opportunities for US adversaries, such as Russia and China, to sneak a hackable vulnerability into those systems that those nations' intelligence services can later exploit."[17] Similar concerns apply to the potential for adversaries to introduce components that are particularly vulnerable to electromagnetic threats into supply chains.

China also dominates the global capacity for IT-related assembly and manufacturing.[18] Many of the hardware products in infrastructure networks likely contain products manufactured in China, which could expose them to potential contamination. As evidence of this potential threat, intelligence officials and legislators raised concerns at a recent congressional hearing about Chinese penetration in the telecom sector—particularly of potential

14 United States Computer Emergency Readiness Team, "Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," *Department of Homeland Security*, last updated March 16, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.

15 "CHRYSENE," *Dragos, Inc.,* May 17, 2018, https://dragos.com/blog/20180517Chrysene.html.

16 "Supply Chain Risk Management: Intelligence.Gov Background Paper," p. 1.

17 Joseph Marks, "DHS to Scrutinize Government Supply Chain for Cyber Risks," *Nextgov*, February 14, 2018, http://www.nextgov.com/cybersecurity/2018/02/dhs-scrutinize-government-supply-chain-cyber-risks/145998/.

18 Lam and Jimenez, "US' IT supply chain vulnerable to Chinese, Russian threats," *The Hill*.

equipment contracts with US government and industry.[19] The United States also banned the use of the Russian firm AO Kaspersky Lab's products from all federal information systems, citing security concerns.[20] Adversaries then could leverage system access for nefarious attacks.

Moreover, potential adversaries are already attempting to subvert SCRM initiatives and will likely do so successfully in the years to come. A prime example is Huawei Technologies. The Chinese ICT firm is a member of several cybersecurity organizations with SCRM-focused initiatives, including the Open Group (and their Open Trusted Technology Provider™ Standard (O-TTPS) Certification Program)[21] and SAFECode (and their Fundamental Practices for Secure Software Development).[22] In addition to direct supply chain threats, it is expected that SCRM initiatives themselves will become potential sources of adversary infiltration efforts.

3. Opacity and complexity of supply chains

As supply chains become more international, they are also becoming increasingly complex. The globalization process has been characterized by "a complex web of contracts and subcontracts for component parts, services, and manufacturing extending across the country and around the world," and the multiple layers and networks of suppliers are frequently not well understood.[23] The National Institute of Standards and Technology, a leading SCRM stakeholder, warns that it is becoming increasingly difficult to vet supply vendors and providers. Indeed, many companies find it challenging to

19 Marks, "Chinese Telecoms Could Join Kaspersky On Government-wide Banned List," *Nextgov*.

20 Department of Homeland Security, "Notification of Issuance of Binding Operational Directive 17-01 and Establishment of Procedures for Responses," *Federal Register* 82, no. 180, September 19, 2017, p. 43782, https://www.federalregister.gov/documents/2017/09/19/2017-19838/national-protection-and-programs-directorate-notification-of-issuance-of-binding-operational.

21 "Standard Open Group Membership," *The Open Group*, last updated June 5, 2018, http://reports.opengroup.org/membership_report_all.pdf.

22 "Members," *SAFECode,* https://safecode.org/members/.

23 "Supply Chain Risk Management: Intelligence.Gov Background Paper," p. 1.

vet supply chain partners beyond the first tier.[24] However, many infrastructure owners and operators depend on a "complex, globally distributed, and interconnected supply chain ecosystem" for products and services, which contain multiple tiers of outsourcing and diverse distribution routes.[25] Meanwhile, adversaries can operate through numerous front companies, organizations, and individuals to hide their presence, obfuscating efforts to discover and counter their actions.[26]

Given the increasing number of vendors and third-party providers upon which power companies rely, "utilities often find it difficult to ensure supply chain integrity."[27] It is possible that potentially compromised products could make their way into infrastructure systems without system owners' knowledge.

4. Convergence of information and operational technology networks

The growing convergence between IT and OT systems increases the potential risks and consequences of a cyberattack. OT systems such as Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) are increasingly prevalent in infrastructure systems. And while these OT systems previously operated on a separate network, segmented from IT networks, the two are increasingly converging.[28] This is creating additional vulnerabilities and increasing systems' attack surfaces. More concerning, however, is that compromised OT systems—especially on a large scale—can have direct physical (and potentially catastrophic) consequences for infrastructure.

---

24 National Institute of Standards and Technology, "Best Practices in Cyber Supply Chain Risk Management: Vendor Selection and Management," n.d., p. 1, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Vendor-Selection-and-Management.pdf.

25 "Cyber Supply Chain Risk Management," *National Institute of Standards and Technology,* last updated April 16, 2018, https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management.

26 Ibid., p. 2.

27 Mission Support Center, Idaho National Laboratory, "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector," August 2016, p. 15, https://bit.ly/2G4OQrH.

28 The Public-Private Analytic Exchange Program, "Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector," p. 4.

Ongoing Industry and Government Progress

Valuable and rapidly-growing SCRM initiatives are underway. Indeed, such initiatives are growing so rapidly that no comprehensive, up-to-date survey of these activities exists. The section that follows provides an initial attempt to offer such a survey. The list is surely not exhaustive, as some initiatives will undoubtedly be overlooked. Nevertheless, the section highlights many of the most important ones.

These SCRM efforts, which may come in the form of standards, best practices, and other regulatory measures, all focus on the same goal: "identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/OT product and service supply chains."[29] SCRM initiatives should address "the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage."[30]

Many of the initiatives examined below assess and attempt to mitigate supply chain risks, sometimes for a particular sector or subset of infrastructure. The section first examines the electricity subsector initiatives. The next subsections outline SCRM initiatives that are multi-sector in nature, along with a new—and potentially very promising—initiative led by Siemens.

Energy Sector Initiatives

The energy sector, and especially the electricity subsector, plays a critical role in enabling all other infrastructure sectors. Threats to this sector are particularly acute, spurring both industry and government efforts to address the multitude of associated challenges. However, efforts to define requirements and further research and development to secure the supply chains for grid technologies is lagging, despite knowledge of adversarial threats and increased risks due to globalized supply chains.[31] Nevertheless, some important initiatives are underway which may form the basis of future efforts.

---

29 "Cyber Supply Chain Risk Management," *National Institute of Standards and Technology.*

30 Ibid.

31 Public-Private Analytic Exchange Program, "Identifying and Mitigating Supply Chain Risks," p. 2.

1. Department of Energy (DOE)

As the sector-specific agency (SSA) for the energy sector, DOE is working to address cyber supply chain vulnerabilities. The department's "Cybersecurity Procurement Language for Energy Delivery Systems" guidance, developed in partnership with industry, provides utilities with "strategies and suggested language to help the US energy sector and technology suppliers build in cybersecurity protections during product design and manufacturing."[32]

DOE also released its "Multiyear Plan for Energy Sector Cybersecurity" in March 2018. Among the plan's goals and objectives is the imperative to "reduce critical cybersecurity supply chain vulnerabilities and risks."[33] To do so, DOE plans to:

> *Identify actions the federal government can take to reduce supply chain risk*: DOE will work with federal partners to identify and take appropriate actions to mitigate supply chain cybersecurity risks and facilitate the building of trust between owners and operators and energy sector ICS manufacturers.
>
> *Develop an energy delivery systems (EDS) testing and analysis laboratory:* As threats continually evolve and new vulnerabilities are discovered and targeted by adversaries, national capabilities are needed to evaluate risk, assess alternative approaches, and engage with other government and private sector cyber analysis capabilities to quickly share actionable information. DOE will establish a robust cyber-physical testing capability at national laboratories to analyze systems and component vulnerabilities, malware threats, and impacts of zero-day threats on energy infrastructure; and to support initiatives to harden the supply chain. This will be accomplished by developing requirements and engaging the National Laboratories and private sector."[34]

The 2018 cybersecurity plan also emphasizes the importance of researching, developing, and demonstrating tools and technologies to help prevent a cyber incident. Specific to SCRM, these tools should aim to "decrease the

32 "Energy Department Releases New Guidance for Strengthening Cybersecurity of the Grid's Supply Chain," *Department of Energy*, April 28, 2014, https://www.energy.gov/articles/energy-department-releases-new-guidance-strengthening-cybersecurity-grid-s-supply-chain.

33 "Multiyear Plan for Energy Sector Cybersecurity," *Department of Energy*, March 2018, p. 6.

34 Ibid., p. 25.

risk posed by malicious functionality that could be inserted as components and systems traverse the supply chain."[35] DOE and its partners are already making progress towards this end. The plan notes that "DOE research partnerships are advancing tools and technologies that help identify undesired, potentially malicious, functionality that may have been inserted in hardware, firmware or software of EDS [energy delivery system] components as they traverse the supply chain; that offer guidance on procurement language that purchasers and suppliers of EDS can use as a starting point to discuss needed cybersecurity measures during the EDS process; and that help ensure the integrity of patches and upgrades."[36]

The DOE strategy also calls for "secure code development and software quality assurance (1.2 and 1.3): Secure and safe coding practices can be implemented on new products, but high cost, conflicts with legacy products, and lack of demand remain key barriers. Significant work is needed in awareness and workforce training. Supply chain risk remains a key issue."[37]

In addition, DOE's response to Executive Order No. 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," issued in May 2017, provides encouraging—although not yet tangible—progress. A DOE report acknowledges the severity of supply chain threats to grid components and urges the department to "develop a national laboratory testing program for examining grid components to assess cybersecurity supply chain posture and examine cyber malware impacts to components in a simulated environment."[38] It is currently unclear how much progress, if any, is underway since DOE recommended the initiative in August 2017.

The department is also working with its national laboratories to conduct its own product testing. The Idaho National Laboratory's (INL) Critical Infrastructure Test Range, which includes "test beds" for the electric grid and other cyber components, "allows for scalable physical and cyber performance testing to be conducted on industry-scale infrastructure systems."[39] DOE is also working with other national laboratories for a variety of cybersecurity-

35 Ibid., p. 34.

36 Ibid.

37 Ibid., p. 45.

38 "Section 2(e): Assessment of Electricity Disruption Incident Response Capabilities," *Department of Energy,* August 9, 2017, p. 29.

39 "Securing the Electrical Grid from Cyber and Physical Threats," *Idaho National Laboratory*, https://www.inl.gov/research-programs/grid-resilience/.

related energy sector projects through the National SCADA Test Bed.[40] In addition, DOE is partnering with a handful of national laboratories (with INL as the lead laboratory), other government stakeholders, and industry on the Cyber Testing for Resilience of Industrial Control Systems (CyTRICS) program, which is currently in the pilot stage. Through CyTRICS, DOE intends to test critical components and leverage the test data to identify systemic and supply chain risks.

2. Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC)

FERC is laying the foundations for private sector SCRM requirements in the electricity subsector. In July 2016, FERC directed NERC to develop SCRM reliability standards.[41] Specifically, FERC charged NERC with developing standards that would require entities to develop an SCRM plan focused on four objectives: "(1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."[42] While they have not yet been subject to enforcement, FERC approved NERC Standards CIP-013-1 (Cyber Security—Supply Chain Risk Management), CIP-005-6 (Cyber Security—Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security—Configuration Change Management and Vulnerability Assessments) in January 2018.[43] Collectively, FERC believes they address the objectives stated above. CIP-013-1, for example, intends to "mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems."[44]

NERC's supply chain reliability standards are extremely valuable for meeting the supply chain risks in the electricity subsector. Moreover, as

---

40 "National SCADA Test Bed," *Department of Energy*, https://www.energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed.

41 "FERC Directs Development of Standards for Supply Chain Cyber Controls," *Federal Energy Regulatory Commission*, July 21, 2016, https://www.ferc.gov/media/news-releases/2016/2016-3/07-21-16-E-8.asp#.WQC2DGnysuU.

42 "Supply Chain Risk Management Reliability Standards (Docket No. RM17-13-000)," *Federal Energy Regulatory Commission,* 162 FERC ¶ 61,044, January 18, 2018, p. 5.

43 Ibid., p. 1.

44 North American Electric Reliability Corporation, "CIP-013-1—Cyber Security—Supply Chain Risk Management," July 2017, p. 3, https://bit.ly/2A1rWyE.

with existing power company initiatives to build resilience against cyber and electromagnetic threats, many companies go above and beyond the requirements of reliability standards and *voluntarily* take additional resilience measures. The same approach makes sense for supply chain security.

While the new standards provide an important baseline for strengthening the electricity subsector's supply chains, they also entail some limitations. For example, due to FERC and NERC's jurisdiction under Section 215 of the Federal Power Act, only certain power industry entities are required to comply with these standards. FERC notes specifically that this does not include "non-jurisdictional suppliers, vendors or other entities that provide products or services to responsible entities."[45] Even among those under FERC and NERC jurisdiction, the standards (with one minor exception) do not apply to Electronic Access Control and Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs), or entities considered "low impact." FERC notes that "there remains a significant cyber security risk associated with the supply chain for BES Cyber Systems" as a result.[46]

3. Electricity Subsector Coordinating Council (ESCC)

The ESCC is a critical link between the subsector's government and industry partners. The body and its leadership play an important role in spurring resilience initiatives and contribute significantly to overall grid security. Among those initiatives, the ESCC is working on supply chain security. Specifically, the ESCC is working with the government to convene public and private sector stakeholders, as well as security and technology vendors, "to identify and share best practices to address threats to the supply chain."[47] The ESCC and DOE are also working toward a data-based program to identify systemic supply chain risks and vulnerabilities.

4. Nuclear Regulatory Commission (NRC)

Nuclear energy entities, not subject to FERC/NERC regulation, have their own cybersecurity guidelines. In particular, the NRC's "Protection

45 Federal Energy Regulatory Commission, "Supply Chain Risk Management Reliability Standards (Docket No. RM17-13-000)," 162 FERC ¶ 61,044, January 18, 2018, p. 7.

46 Ibid., p. 3 and 8.

47 "ESCC," *Electricity Subsector Coordinating Council*, January 2018, http://www.electricitysubsector.org/ESCCInitiatives.pdf?v=1.8.

of digital computer and communication systems and networks" lays out cybersecurity requirements for complying entities.[48] Those requirements broadly require entities to ensure the protection of their systems, and do not entail specific SCRM provisions. However, (d)(3) requires entities to "ensure that modifications to assets . . . are evaluated before implementation," which could address vulnerabilities introduced by software and hardware updates. The NRC's regulatory guidance from 2010 does explicitly note the need for SCRM among their operational and management security controls. NRC recommends that facilities protect against supply chain threats and vulnerabilities by establishing trusted distribution paths, validating vendors, and requiring that acquired products are tamper-proof (or have tamper-evident seals).[49] NRC plans to review its cybersecurity regulations in 2019 and update as necessary.[50]

Multi-Sector Initiatives

1. Department of Homeland Security (DHS)

DHS is augmenting its SCRM efforts. DHS established its Cyber Supply Chain Risk Management (C-SCRM) program in January 2018 to serve as the "lead organization and central coordination point for whole-of-government C-SCRM."[51] The initiative has an ambitious vision of enabling "a national and global ICT market and operational environment where the existence of intentionally and negligently misconfigured, poorly manufactured, and counterfeit hardware, components, and software is readily identified, actionable through interdiction or mitigation, and rare."[52] DHS also outlined the program's major activities to:

- establish a supply chain risk assessment capability to serve stakeholders

48 US Nuclear Regulatory Commission, "§ 73.54 Protection of digital computer and communication systems and networks," 2009, https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html.

49 US Nuclear Regulatory Commission, "Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities," January 2010, pp. C-29–C-30, https://www.nrc.gov/docs/ML0903/ML090340159.pdf.

50 Sean Lyngaas, "Nuclear Power Plants Have a 'Blind Spot' for Hackers. Here's How to Fix That," *Motherboard*, April 27, 2018, https://motherboard.vice.com/en_us/article/mbxy33/cyberattacks-nuclear-supply-chain.

51 Department of Homeland Security, "Cyber Supply Chain Risk Management: Becoming a Smarter Consumer of ICT in a Connected World," June 2018, p. 15.

52 Ibid.

- establish a communications, notification, and information-sharing capability among stakeholders
- establish qualified bidder and manufacturer lists through implementing a robust process for validating and approving the security practices of companies and the security characteristics of ICT products and services
- provide stakeholders with assistance in developing and implementing supply chain risk management capabilities.[53]

The C-SCRM imitative, which includes General Services Administration (GSA), the Department of Defense (DOD), the intelligence community, and private sector stakeholders, is intended to help inform government procurement decisions.[54] According to a DHS official, the initiative will "provide actionable information about supply chain risks and mitigations to users, buyers, manufacturers and sellers of tech products. It will also identify risks to federal networks and other national or global stakeholders."[55] Assistant Secretary for the Office of Cybersecurity and Communications at the National Protection and Programs Directorate (NPPD) Jeanette Manfra further noted that the C-SCRM initiative will "identify and mitigate supply chain threats and vulnerabilities" to high-value assets.[56]

The initiative builds on valuable, existing DHS tools for addressing supply chain risks. The Continuous Diagnostics and Mitigation (CDM) program, for example, contains an acquisition strategy to mitigate supply chain-based cyber threats. This strategy includes the Approved Products List (APL), an "authoritative product catalog that has been approved to meet CDM technical capability requirements."[57] Through the CDM/APL, DHS also has a specific SCRM plan, the objective of which is to "provide information to Agencies

53 Ibid., p. 16.

54 Jory Heckman, "DHS, Lawmakers Doubling down on Supply Chain Risk Management," *Federal News Radio,* February 15, 2018, https://federalnewsradio.com/cybersecurity/2018/02/dhs-lawmakers-doubling-down-on-supply-chain-risk-management/.

55 Lauren C. Williams, "DHS Developing Supply Chain Security Initiative," *FCW,* February 14, 2018, https://fcw.com/articles/2018/02/14/dhs-supply-chain-security.aspx.

56 *US House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Technology* (2018) (statement of Jeannette Manfra, Assistant Secretary for Cybersecurity and Communications, NPPD), DHS, p. 8.

57 "Continuous Diagnostics and Mitigation (CDM)," *Department of Homeland Security*, last updated February 22, 2018, https://www.dhs.gov/cdm.

and ordering activities about how the offeror identifies, assesses, and mitigates supply chain risks in order to facilitate better informed decision-making by Agencies and ordering activities."[58]

2. National Institute of Standards and Technology (NIST)

NIST is a leading source of SCRM guidance. NIST's Computer Security Resource Center (CSRC) has a major Cyber Supply Chain Risk Management program. Notably, the CSRC recognizes the supply chain threats to IT and OT networks.[59] NIST's 2015 SCRM publication provides comprehensive guidance on managing cyber supply chain risks. The guidelines provide a framework for federal departments and agencies which "can be modified or augmented with organization-specific requirements from policies, guidelines, and other documents."[60] The document presents a set of processes and measures for evaluating and managing supply chain risk and provides a template for developing SCRM plans. NIST also provides a set of SCRM best practices applicable to all infrastructure sectors.[61] Moreover, NIST's updates to their "Framework for Improving Critical Infrastructure Cybersecurity" (Cybersecurity Framework) in 2017 included "new details on managing cyber supply chain risks,"[62] while the April 2018 update includes further revisions on "managing cybersecurity within the supply chain."[63]

In addition to these initiatives and guidelines, NIST convenes leaders from government, the private sector, and academia to address supply chain

58 Government Services Agency, "Continuous Diagnostics and Mitigation (CDM) Approved Products List (APL) Supply Chain Risk Management (SCRM) Plan," August 2017, p. 1.

59 "Cyber Supply Chain Risk Management," *National Institute of Standards and Technology.*

60 National Institute of Standards and Technology "Supply Chain Risk Management Practices for Federal Information Systems and Organizations (SP 800-161)," April 2015, p. 2.

61 National Institute of Standards and Technology, "Utility Sector Best Practices for Cyber Security Supply Chain Risk Management," October 2015, https://www.nist.gov/sites/default/files/documents/itl/csd/USRP_NIST-Utility_100115.pdf.

62 "NIST Releases Update to Cybersecurity Framework," *National Institute of Standards and Technology*, January 10, 2017, https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework.

63 "NIST Releases Version 1.1 of its Popular Cybersecurity Framework," *National Institute of Standards and Technology*, April 16, 2018, https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework.

risks. The Software and Supply Chain Assurance Forum, co-led by DHS, GSA, and DOD, allows participants to "share their knowledge and expertise regarding software and supply chain risks, effective practices and mitigation strategies, tools and technologies, and any gaps related to the people, processes, or technologies involved."[64]

This sharing and coordination function is helpful; however, it falls drastically short of need. It would be incredibly expensive and altogether impractical to assume that individual participants in this process would develop their own product certification mechanisms, fully share their conclusions with their colleagues, and create the unified "demand pull" needed to grow the supply of certified products.

3. Office of Management and Budget (OMB)

The OMB provides a key source of federal government cybersecurity policy. Indeed, the Federal Information Security Modernization Act (FISMA) requires the OMB to oversee agency information security policies and practices. The "OMB Circular A-130: Managing Information as a Strategic Resource," issued in 2016, establishes "general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources and supporting infrastructure and services" for the executive branch of the federal government.[65] A-130 contains the primary guidance to such agencies for implementation of FISMA and includes some guidance for federal SCRM. Particularly, the document states that agencies shall:

- "consider . . . supply chain security issues for all resource planning and management activities throughout the system development life cycle so that risks are appropriately managed;"
- "analyze risks (including supply chain risks) associated with potential contractors and the products and services they provide."[66]

64 "Software and Supply Chain Assurance Forum," *National Institute of Standards and Technology*, last updated March 29, 2018, https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management/SSCA.

65 Office of Management and Budget, "Circular No. A-130: Managing Information as a Strategic Resource," July 2017, p. 6, https://bit.ly/2rAjz7Q.

66 Ibid., p. 6 and 11.

An Appendix to A-130 which "establishes minimum requirements for federal information security programs" also requires agencies to:

- "implement supply chain risk management principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, as well as poor manufacturing and development practices throughout the system development life cycle;"
- "develop supply chain risk management plans as described in NIST SP 800-161 to ensure the integrity, security, resilience, and quality of information systems."[67]

If implemented and stringently verified, the A-130 could contribute to the security of executive branch supply chains. However, the policy provides little in terms of specific requirements, other than deferring to the NIST guidance examined above. It also requires each agency to create their own SCRM program, which—as noted throughout—is not economically feasible to achieve at the required level of comprehension.

Moreover, while the policy applies to the majority of Sector-specific agencies (SSA) (except, critically, the Environmental Protection Agency as SSA for the water and wastewater sector), it is limited to only a subset of government agencies and does not apply to industry or other stakeholders.

4. General Services Administration (GSA)

GSA plays a key role in federal government acquisition and, accordingly, in securing federal IT supply chains. Specifically, GSA is "establishing a comprehensive SCRM capability that will ensure government agencies procure IT hardware and software from original equipment manufacturers, including authorized resellers or other trusted sources."[68] They are also establishing a Vendor Risk Assessment Program (VRAP) to "evaluate known or potential risks related to suppliers of products and services."[69]

---

67 Ibid., p. 40 and 42.

68 Shon Lyublanovits, "Reducing Cybersecurity Risks in Supply Chain Risk Management," *General Services Administration*, September 18, 2017, https://gsablogs.gsa.gov/technology/2017/09/18/reducing-cybersecurity-risks-in-supply-chain-risk-management/.

69 Ibid.

5. Office of the Director of National Intelligence (ODNI) and the National Counterintelligence and Security Center (NCSC)

ODNI has produced SCRM policy for the intelligence community. Intelligence Community Directive 731, in particular, is the policy "to protect the supply chain as it relates to the lifecycle of mission-critical products, materials, and services used by the IC through the identification, assessment, and mitigation of threats."[70] It is supplemented by specific directives on determining the mission criticality of components, details on conducting threat assessments, and improving information sharing.

In addition to the directives, ODNI's NCSC also has highlighted SCRM threats. A 2013 white paper and 2017 backgrounder provide succinct yet valuable introductions to cyber supply chain threats and risk management.[71] In cooperation with DHS, NCSC also launched an industry partnership that is contributing to SCRM efforts. The Public-Private Analytic Exchange Program (AEP) first identified cyber SCRM risks as a major focus for the electricity subsector in a 2016 white paper. The report offers key SCRM findings and recommendations for both industry and government.[72] A more detailed report from 2017 builds on that white paper to provide more comprehensive recommendations, specifically regarding OT threats. AEP produced the report to "highlight potential security risks to the SCADA supply chain in the current nascent stage to prevent an expensive, future retrofit of an established industry."[73]

While the report is still largely an information product with recommendations rather than a detailed basis for concrete action, it nevertheless provides extremely valuable context and highlights the NCSC—and the AEP in particular—as a potentially valuable partner for CPIC. This is especially true since implementing the recommendations of the AEP report of having companies build their own certification mechanisms and create the market forces necessary to grow the supply of certified hardware and software is untenable.

---

70 Office of the Director of National Intelligence, "Intelligence Community Directive 731 – Supply Chain Risk Management," December 2013, p. 1.

71 NCSC, *Supply Chain Risk Management: Framework for Assessing Risk*.

72 Public-Private Analytic Exchange Program, "Identifying and Mitigating Supply Chain Risks."

73 Ibid., p. iii.

6. Department of Defense (DOD)

DOD also has an SCRM policy to achieve "trusted" systems and networks. Last updated in July 2017, DOD Instruction 5200.44 "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks" establishes policies to minimize the risks related to "vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components . . . by foreign intelligence, terrorists, or other hostile elements."[74] The instruction emphasizes the importance of managing supply chain risks through the entirety of a product's lifecycle. This policy is specific to DOD's mission-critical functions, although similar principles and approaches can be applied to the CPIC's efforts and general approach.

7. White House

The White House emphasizes the importance of securing global supply chains in two separate initiatives. To manage supply chain risks the "National Strategy for Global Supply Chain Security," issued in January 2012, calls for a greater understanding of supply chain threats that stem from "exploitation of the system by those seeking to introduce harmful products or materials."[75] The White House's Comprehensive National Cybersecurity Initiative also highlights supply chain threats. Initiative 11 is to "develop a multi-pronged approach for global supply chain risk management," in which managing risks will involve "the development and employment of tools and resources to technically and operationally mitigate risk across the lifecycle of products (from design through retirement) . . . and partnership with industry to develop and adopt supply chain and risk management standards and best practices."[76]

Private Sector Initiatives

One private sector initiative is particularly promising and deserving of consideration: the Charter of Trust Initiative. Siemens recently joined with the Munich Security Conference and other governmental and business partners (including IBM and AES) to launch this initiative. The charter is intended

74 Department of Defense, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," Instruction No. 5200.44, last updated July 27, 2017, p. 1.

75 White House, "National Strategy for Global Supply Chain Security," January 2012, p. 4.

76 White House, "The Comprehensive National Cybersecurity Initiative," March 2010, https://obamawhitehouse.archives.gov/node/233086.

to "develop and implement rules for ensuring cybersecurity throughout the networked environment."[77]

Principle 7 of the charter offers a possible focus for dialog with Siemens and its charter partners. This principle states that "companies—and if necessary—governments establish mandatory independent third-party certifications (based on future-proof definitions, where life and limb is at risk in particular) for critical infrastructure as well as critical IoT solutions."[78] This provides an opportunity for CPIC to partner with Charter of Trust participants on collaborative SCRM solutions that leverage each initiative's strengths and resources.

Product Certification

Product certification-focused organizations and initiatives exist, largely in the private sector, to assess potential risks to specific products, processes, and systems. A significant number of these organizations and certification schemes exist worldwide, although only a few are surveyed here. Many of these certification bodies include considerations for cybersecurity, although few certify for electromagnetic thresholds.

1. Underwriters Laboratories (UL)

UL provides a wide array of certification services, ranging from specific products, facilities, processes, or systems to industry-wide standards and requirements.[79] As an industry leader in the United States, working with manufacturers, industry experts, other testing labs, and governments, UL testing standards are often considered the "de facto standards of the US government."[80] UL can also serve as an independent third party to certify

77 "Time for Action: Building a Consensus for Cybersecurity," *Siemens,* May 17, 2018, https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/cybersecurity-charter-of-trust.html.

78 "Charter of Trust: For a Secure Digital World," *Charter of Trust,* February 2018, https://www.siemens.com/press/pool/de/feature/2018/corporate/2018-02-cybersecurity/charter-of-trust-e.pdf.

79 "Certification," *Underwriters Laboratories,* https://services.ul.com/categories/certification/.

80 Mike Murphy, "Inside the 122-year-old Company that Makes Sure our Electronics Don't Blow up our Homes," *Quartz*, April 5, 2016, https://qz.com/643007/inside-the-122-year-old-company-that-makes-sure-our-electronics-dont-blow-up-our-homes/.

supply chains and related processes.[81] The US Department of Labor's Occupational Safety and Health Administration considers UL as one of its Nationally Recognized Testing Laboratories.[82]

2. International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

ISO and IEC are two separate entities that cooperate to create industry and product standards and certification. Specifically, the ISO/IEC Joint Technical Committee (JTC) 1 focuses on standards development for IT.[83] ISO/IEC standard 27036, of which there are four parts, provides guidelines "to assist organizations in securing their information and information systems within the context of supplier relationships."[84] Outside of this joint work, the IEC also develops electromagnetic standards, including those for "complex products or those that operate in a special environment."[85]

The IEC's 62443 series of standards offer an especially useful model for further analysis. These standards address the need to design cybersecurity robustness and resilience into industrial automation control systems (IACS). In particular, the 62443-4-1 standard describes the derived requirements that are applicable to the development of control system products.[86] The ISO/IEC standards can help inform the criteria for future certification schemes, although further outreach will be necessary to determine the extent to which (and how) ISO/IEC provides continuing testing and verification of products and vendors.

---

81 "Supply Chain Certification," *Underwriters Laboratories*, https://services.ul.com/service/supply-chain-certification/.

82 "Current List of NTRLs," *Occupational Safety and Health Administration*, https://www.osha.gov/dts/otpca/nrtl/nrtllist.html.

83 "ISO/IEC JTC 1 — Information Technology," *International Organization for Standardization*, https://www.iso.org/isoiec-jtc-1.html.

84 "ISO/IEC 27036-1:2014," *International Organization for Standardization*, April 2014, https://www.iso.org/standard/59648.html.

85 "EMC Product Standards," *International Electrotechnical Commission*, 2018, http://www.iec.ch/emc/emc_prod/.

86 "Overview – The 62443 Series of Standards," *ISA, 2015*, https://fr.scribd.com/document/358894928/ISA-62443-Series-Overview.

3. The SAFETY Act (DHS)

DHS has a product certification scheme for anti-terrorism technologies. In the wake of the 9/11 attacks, the private sector was "extremely reluctant to deploy security technologies and services in civilian settings due to the enormous liability risks involved."[87] These companies would be liable if their product did not stop or mitigate the attack it was designed to prevent. In response, Congress enacted the Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act) in 2002 "to ensure that the threat of liability does not deter potential manufacturers or sellers of effective anti-terrorism technologies from developing and commercializing technologies that could save lives."[88] The SAFETY Act contains a mechanism to certify a broad range of products, services, and technologies as Qualified Anti-Terrorism Technologies (QATT), placing them on the Approved SAFETY Act Product List for Homeland Security.[89] DHS grants liability limitations for the sellers and users of such QATTs.[90] Among the products currently approved for SAFETY Act liability protections are cybersecurity technologies.[91]

4. International Cybersecurity Certification Programs

A number of certification mechanisms and bodies exist to ensure the cybersecurity of products. Indeed, tiered security certification for commercial IT products has existed for over thirty years.[92] The criteria that inform these certification schemes have been enshrined in standards, such as the Common Criteria (CC). CC has also established an extensive certification arrangement, which includes a product certification scheme. The objectives of this arrangement include ensuring the high-quality evaluation of IT products, improving the availability of certifiably secure products, eliminating the burden of duplicate evaluations, and continuously improving "the efficiency

87 Department of Homeland Security, "Research and Development Partnerships – SAFETY Act for Liability Protection," January 14, 2014, https://bit.ly/2JPIolm.

88 Department of Homeland Security, "The Office of SAFETY Act Implementation," https://www.dhs.gov/science-and-technology/safety-act.

89 Department of Homeland Security, "Research and Development Partnerships – SAFETY Act for Liability Protection," January 14, 2014, https://bit.ly/2JPIolm.

90 Ibid.

91 Ibid.

92 Steven B. Lipner, *SAFECode Perspective on Cybersecurity Certification*, January 2018, p. 1, https://safecode.org/wp-content/uploads/2018/02/SAFECode_Perspective_on_Cybersecurity_Certification.pdf.

and cost-effectiveness of the evaluation and certification/validation process."[93] CC has certified 2,351 products as of June 5, 2018, which include access control devices and systems, operating systems, detection devices and systems, and boundary protection devices and systems.[94]

As with many cybersecurity-focused (rather than specifically infrastructure-focused) initiatives, one potential flaw lies in the CC's focus on IT rather than OT. In addition, its membership does not include any participation from China, Russia, or any other near-peer cyber adversaries.[95] The membership structure, however, does include a management committee with senior representatives from each signatory country "to implement the Arrangement and to provide guidance to the respective national schemes conducting evaluation and validation activities."[96]

A range of other public and private sector cybersecurity certification programs exist. As mentioned above, some SCRM initiatives may be inherently compromised by the membership of their founding organization. While the Open Group boast an international membership of over 500, with an extremely large US contingent, this organization extends to the point of including potential adversaries. SAFECode's membership is much smaller, but nevertheless includes the same potential adversary.

a. SAFECode

The SAFECode program, a software assurance-focused, EU-based organization, has a similar vision to CPIC. SAFECode is looking to help users "identify products and online services that provide effective security and can incentivize suppliers to invest in effective security—and help to ensure that they are rewarded for that investment."[97] Notably, SAFECode is helping the small and mid-sized organizations that are struggling to keep up with major organizations worldwide, which have funded their own SCRM programs.[98]

---

93 "About the Common Criteria," *Common Criteria*, https://www.commoncriteriaportal.org/ccra/index.cfm.

94 "Certified Products," *Common Criteria*, https://www.commoncriteriaportal.org/products/.

95 "Members of the CCRA," *Common Criteria*, https://www.commoncriteriaportal.org/ccra/members/.

96 "About the Common Criteria," *Common Criteria*.

97 Lipner, *SAFECode Perspective on Cybersecurity Certification*, p. 2.

98 Ibid., p. 3.

CPIC addresses this challenge by centralizing the resources required to secure supply chains and by creating a strong, consistent "demand signal" for the production of secure products.

SAFECode's backgrounder on cybersecurity certification provides a number of important perspectives. Critically, SAFECode emphasizes the importance of certifying a product while it is being developed—rather than after it is released for sale—to ensure that companies do not rely on a product with potential vulnerabilities while certification is pending.[99] Moreover, in highlighting the value of a tiered certification system, SAFECode notes that "schemes that provide varying levels of certification incentivize developers to seek the highest levels of certification."[100] In addition, SAFECode underscores the inherent international footprint of today's supply chains, urging "broad mutual recognition in order to provide maximum benefit to users and developers worldwide."[101]

SAFECode has limitations for infrastructure SCRM as its sole focus is on IT (rather than OT) products. SAFECode also appears to place the onus for compliance, testing, and verification on the organizations themselves, which leads to a drastic duplication of resources and other inefficiencies. SAFECode's "Fundamental Practices for Secure Software Development" can nevertheless provide an additional source of insights for future certification programs.[102]

b. O-TTPS Certification Program

The Open Group O-TTPS program includes guidelines, recommendations, requirements, and best practices aimed at "enhancing the integrity of [commercial off-the-shelf and communication technology] products and the security of their global supply chains."[103] The Open Group certifies

99 Ibid., p. 2.

100 Ibid.

101 Ibid.

102 SAFECode, "Fundamental Practices for Secure Software Development: Essential Elements of a Secure Development Lifecycle Program (Third Edition)," March 2018, https://safecode.org/wp- content/ uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf.

103 "The Open Trusted Technology Provider Standard (O-TTPS) Certification Program," *The Open Group*, http://www.opengroup.org/certifications/o-ttps.

organizations that they deem to comply with the program requirements as "Open Trusted Technology Providers."[104]

O-TTPS policy and guidance documents can also provide important foundational material for future initiatives. The 2017 certification policy document, for example, includes detailed workflow diagrams for third-party certification, with additional detail for each step of the process.[105] The document also includes specific policies for conformance requirements, maintaining certification, re-certification, and an appeal process for certification decisions, among others.

The CPIC Initiative

The Cyber Product International Certification (CPIC) initiative proposed by the EIS Council will help meet many of the challenges outlined above. At present, infrastructure owners and operators lack a compressive, stakeholder-driven process to certify that crucial hardware and software products are even minimally scrubbed of malware and other means of adversary exploitation. Establishing such a certification process would make an enormous contribution to cyber resilience, especially if government agencies can provide threat information and other forms of support for the initiative. CPIC could also meaningfully contribute to infrastructure resilience by including measures to certify products against intentional electromagnetic interference (IEMI). Key issues for consideration in developing the CPIC initiative are:

1. Leveraging existing company plans and capabilities for SCRM

Many private sector entities already have procurement guidelines that constitute potential best practices. While the degree to which these best practices are implemented may vary, they nevertheless can form an important foundation for developing the CPIC initiative. Moreover, just as important, these companies have already developed a business case to strengthen their supply chain security and—in many cases—pay more for products that are more secure. Capturing these best practices would be extremely valuable.

104 Ibid.

105 See The Open Group, "Open Trusted Technology Provider Standard (O-TTPS) Certification Policy (Version 1.1)," January 2017, pp. 14–18, https://ottps-cert.opengroup.org/sites/ottps-cert.opengroup.org/files/doc/O-TTPS_Certification_Policy.pdf.

2. Centralized coordination

Internal SCRM models often require each organization to develop and implement their own certification processes for the products and suppliers they use. The cost of doing so—especially when considering the resources required for implementation and verification—can be significant for each individual organization. With CPIC, however, these costs would be proportionally split among participants, drastically reducing the current duplication of effort and resources, and incentivizing and enabling far more comprehensive certification and validation processes than those considered practical today.

3. Guarding against "minimalist" standards

Although they are helpful, standards that constitute the minimum required SCRM measures are not sufficient to ensure the security of global supply chains. Rep. Langevin has urged that "rather than having just a compliance-based mindset that encourages doing the bare minimum," we should "properly incentivize organizations to take a risk-based approach to cybersecurity," including SCRM.[106] Similarly, the AEP urges government and industry to "incentivize business and economic development in response to supply chain security shortfalls," moving away from a reactive cybersecurity model to a more proactive one that "acknowledges and mitigates inherent and potentially introduced supply chain risks."[107]

To address growing SCRM threats, CPIC should employ a non-regulatory approach, focused on certification of best practices rather than minimalist, broad-brush standards. To be sure, the regulatory measures examined in this brief all provide an essential foundation for CPIC's envisioned capabilities and structure. However, CPIC should not replace these standards as a means of securing supply chains. Rather, the initiative is meant to provide companies with trusted, best-in-class options for ensuring supply chain integrity.

Avoiding a standards-based model will also help CPIC refrain from calcifying into a regulatory structure that defeats its best practice intent. Regulatory requirements inevitably move far slower than the threats they are designed to address and also rarely represent best practices. While the CPIC

106 Lauren C. Williams, "DHS Developing Supply Chain Security Initiative," *FCW*, February 14, 2018, https://fcw.com/articles/2018/02/14/dhs-supply-chain-security.aspx.

107 Public-Private Analytic Exchange Program, "Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector," p. 2.

initiative should be compatible with regulatory schemes and requirements, it will be most effective if it is not constrained by them. Ideally, all CPIC certification processes will also have built-in sunset provisions that require periodic reevaluation and updates to meet the newest assessments of evolving threats.

4. Internationalizing CPIC from the start

The vast majority of contemporary supply chains have an international footprint. Yet, most regulatory standards and guidelines are country-specific. For example, with the exception of the Charter of Trust and cybersecurity-specific certification programs, all of the initiatives and models examined in this report are exclusively focused on the United States (though the NERC standards apply to registered bulk power system entities in Canada and Mexico). However, the United Kingdom, Israel, and the other nations also have cutting-edge SCRM initiatives underway that would be valuable to incorporate. Internationalizing the CPIC effort can help create and expand the necessary customer and product user base as well. Supply chain exploitation efforts by Russia, China, and other nations are multi-sector and global in nature. The CPIC initiative should be structured accordingly.

5. Tiered system

The CPIC Commission should consider developing a tiered product certification system. Such a layered structure could include: (1) a Basic Level, above current regulatory standards but not quite "best-in-class" requirements; and (2) the Prime Certification that sets the standard for best-in-class requirements. In fact, by leveraging the market incentives that would be created by many thousands of secure product customers across multiple sectors, this "Prime Certification" level might even become a "better than best-in-class" certification capability.

6. Role of government

While CPIC will be industry-driven, government participation can ensure that the CPIC initiative: (1) can benefit from senior leaders' expertise; (2) will be maximally compatible with participating government stakeholders' own needs; (3) has inherent credibility with those stakeholders; (4) can be integrated seamlessly with existing government initiatives; and (5) incorporates

government priorities to reduce costs. Incorporating government officials from multiple participating countries will provide added benefit by integrating a range of approaches and perspectives but could also create challenges given the disparate levels of influence each government may have on domestic private sector companies.

Conclusion

Reports by the US intelligence community, DHS, DOE, and other agencies highlight the degree to which supply chain exploitation efforts are metastasizing and becoming ever more difficult to detect.

In the electricity subsector and beyond, industry and government are partnering on aggressive, much-needed efforts to manage supply chain risks. CPIC should avoid "re-inventing the wheel" and replicating work that is already underway. Instead, the initiative should be structured to support and fill gaps between these ongoing programs, in ways that are uniquely possible through the CPIC structure and provide the greatest benefits for infrastructure resilience. This report provided a brief overview of ongoing efforts to facilitate future discussions and identify areas where CPIC can make the most meaningful contributions.

Infrastructure owners and operators are also increasingly focused on buying products that are malware-free. By establishing a private sector-founded and sanctioned product certification process developed in coordination with government agencies, and by purchasing products that meet its standards, owners and operators can help bolster the emerging standards and market forces essential to improve SCRM.