SECURING CRITICAL SUPPLY CHAINS

STRATEGIC OPPORTUNITIES FOR THE CYBER PRODUCT INTERNATIONAL CERTIFICATION (CPIC™) COMMISSION INITIATIVE

EIS COUNCIL

Paul Stockton // June 19, 2018

SECURING CRITICAL SUPPLY CHAINS

STRATEGIC OPPORTUNITIES FOR THE CYBER PRODUCT INTERNATIONAL CERTIFICATION (CPIC™) COMMISSION INITIATIVE

Paul Stockton[1]

June 19, 2018

EIS COUNCIL

1 Dr. Paul Stockton, the author of this study, is the Managing Director of SONECON, and a former U.S Assistant Secretary of Defense for Homeland Defense and America's Security Affairs. Robert Denaburg, Senior Analyst at Sonecon, performed research for the report.

Executive Summary

China, Russia and other potential adversaries are ramping up their efforts to corrupt the supply chains on 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 U.S. 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 U.S. security partners.

The Cyber Product International Certification (CPIC™) Commission initiative proposed by the EIS Council will help meet these challenges in an especially important way. 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 add still greater value for infrastructure resilience by including measures to certify products against intentional electromagnetic interference (IEMI). While cyber and IEMI threat vectors are very different, the governance mechanisms, certification processes, and stakeholder-driven strategies that CPIC will need to build to meet cyber challenges can also be adapted to strengthen supply chain resilience against IEMI threats.

However, building a collaborative certification process will require the CPIC Commission to address key impediments. During the EIS Council London Summit, participants will have an opportunity to examine these impediments and build consensus on how to overcome them. The analysis that follows is structured to support consensus-building by examining four critical issues:

1. **The nature of the threat and implications for CPIC priorities and processes**

   Reports by the U.S. intelligence community, the Department of Homeland Security (DHS), the Department of Energy (DOE), and other agencies highlight the degree to which supply chain exploitation efforts are metastasizing and becoming ever-more difficult to detect. Section I of this paper examines recent trends in the threat and suggests some options for prioritizing product certification initiatives. This section also addresses the risk that, as fast as a CPIC Commission process can certify products, adversaries will seek to corrupt them -- perhaps even on a targeted basis.

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.

2. Alignment with and support for ongoing SCRM programs

In the electricity subsector and beyond, industry and government are partnering on aggressive, much-needed efforts to manage supply chain risks. These SCRM efforts, which may come in the form of standards, best practices, and other regulatory measures, are all focused 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. It covers 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."[2]

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. To assist the discussion of these options, Section II provides a first-ever survey of current private and public sector SCRM efforts. Section II also identifies potential partners for developing CPIC, including the Siemens-led Charter of Trust initiative.

3. Leveraging other models of product certification

The Underwriters Laboratories (UL), the International Electrotechnical Commission (IEC), and other product standard-setting and certification organizations provide lessons learned for CPIC efforts to secure products against supply chain exploitation. Section III highlights some prominent models for consideration, and also discusses unique challenges that must be addressed in securing critical products against adversary corruption.

4. Building a "business case" for CPIC and creating a stakeholder-driven governance framework

While government procurement requirements are essential for helping government agencies and Defense Industrial Base companies defeat attacks on their supply chains, government mandates alone cannot meet the needs of infrastructure owners and operators. Instead, CPIC should establish a voluntary, "demand-driven" business model to incentivize vendors to secure at least selected portions of their hardware and software product portfolios against corruption.

2 "Cyber Supply Chain Risk Management," National Institute of Standards and Technology, last updated April 26, 2018, https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management.

Infrastructure owners and operators are 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. Section IV offers preliminary options for Summit participants to discuss for developing such an incentives-based ecosystem.

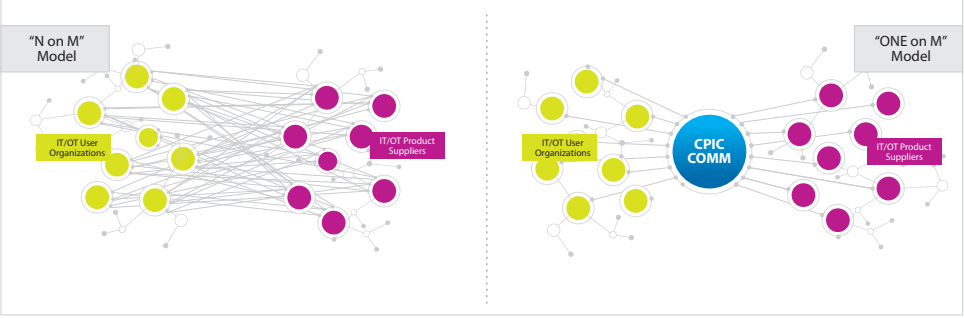

Figure 1 - Advantages of CPIC's Centralized Model

A prerequisite for the success of such a business model will be for major companies to shape the certification process to meet their own priorities, and adjust their spending criteria and acquisition systems to reward vendors who meet the standards that the CPIC Commission will establish. Senior government leaders will also need to contribute to the CPIC development process to ensure that the initiative benefits from their knowledge and expertise, to give CPIC inherent credibility within government departments and agencies, and to make CPIC seamlessly compatible with public sector needs.

However, the current landscape of industry and government standards and guidelines is not sufficient to secure global supply chains against increasingly severe threats. A key finding of this report:

mandatory standards are valuable, they provide only a starting point to build a system of shared best practices in which market forces provide incentives to go above and beyond such minimalist standards.

Moreover, from a business case perspective, it is inefficient and not economically feasible for each company to build their own highly effective SCRM controls. Instead, CPIC can provide a centralized, coordinated system that – once its foundations are developed – can be modularized for any sector or industry. This system might also contain a tiered certification scheme that would not be otherwise financially achievable. Shifting from the current "N on M" SCRM ecosystem to the "ONE on M" model (see Figure 1) enables a range of new security options.

Internationalizing the CPIC effort can help create and expand the necessary customer

base. Supply chain exploitation efforts by Russia, China, and other nations are multi-sector and global in nature. The CPIC Commission initiative should be structured accordingly. The certification process should focus on securing internationally-sourced hardware and software products that are most vital for the critical functions of key sectors in all participating nations, including those products essential to sector-by-sector Black Sky sustainment and restoration operations.[3] That process should also be created through voluntary collaboration between owners and operators of all of these sectors, and their government partners, by the United States and its security partners. Section IV proposes some options on how such broad collaboration might be built and examines the potential benefit of increasing the customer base for CPIC-certified software and hardware.

3 See, for example, the EPRO Sector Black Sky Playbooks. "The EPRO® ESC Sector," EIS Council, n.d.a., https://www.eiscouncil.org/EPRO_ESC_Sector.aspx.

1

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.[4] 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 U.S. and partner networks. This section examines the ways in which supply chain exploitation challenges are intensifying. The section also examines the implications of these challenges for prioritizing CPIC development efforts.

In DHS' 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."[5] 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 SCRM challenges.[6] Despite the current array of public and private sector programs to mitigate and counter supply chain threats, "the evolution of directed, sophisticated and multifaceted threats threatens to outpace our countermeasures."[7] Given the current

4 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.

5 Department of Homeland Security, Cybersecurity Policy, May 15, 2018, p. 1.

6 DHS, Cybersecurity Policy, pp. 22-23.

7 NCSC, Intelligence.Gov Background Paper, p. 2.

threat environment and global supply chain trends, "cyber SCRM is not optional."[8]

Over time, the CPIC initiative will also pursue opportunities to mitigate electromagnetic supply chain threats. 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. A number of factors and trends are intensifying such threats, which the CPIC Commission initiative will have to account for. This intensification of supply chain threats will pose both 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.[9] New IT initiatives such as cloud computing and the Internet of Things have also expanded the cyber supply chain attack surface,[10] increasing the number of potential infiltration points adversaries can target – and creating additional challenges for infrastructure owners and operators trying to secure their supply chains.

Adversaries are seeking opportunities to corrupt every point in the global supply chains that support U.S. infrastructure. There are potential risks at each stage: design, manufacturing, integration, deployment, and maintenance.[11] Adversaries may insert vulnerabilities into the supply chain themselves, or can potentially capitalize on latent,

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

9 NIST, Best Practices in Cyber Supply Chain Risk Management, p. 1.

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

11 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.

inherent vulnerabilities yet to be addressed by security practitioners.[12]

Even if a vulnerability does not exist in initial development, adversaries can insert them at any point in the lifecycle of a system.[13] This includes software updates or vulnerability-correcting "patches" for IT or OT systems which can upload malicious code into a system, or insert malignant firmware for exploitation at a later date.[14] 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, the Defense Science Board (DSB) notes 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" which may be discovered only years after the product enters into service – if at all – and potential effects range from system degradation to system failure.[15]

Software updates are especially prone to hostile efforts to gain persistent access to CI networks, which adversaries could later use to launch disruptive attacks on infrastructure operations. For example, the Russian Dragonfly campaign initially targeted "peripheral organizations such as third-party suppliers with less secure networks," using them as staging targets to pivot to intended victims.[16] ICS cybersecurity firm Dragos, Inc. also recently profiled a threat actor which has been seen to target ICS networks, including through the use of watering hole attacks, to steal credentials and gain access to compromised victims' networks and machines.[17]

2. Covert ownership and globalization of supply chain vendors

Supply chains are becoming increasingly global. As supply chains become increasingly intricate and international, the most capable U.S. adversaries "can access this supply chain at multiple points, establishing advanced, persistent, and multifaceted subversion."[18]

12 Public-Private Analytic Exchange Program, Identifying and Mitigating Supply Chain Risks in the Electricity Infrastructure's Production and Distribution Networks, 2016, p. 4.

13 Defense Science Board, Task Force on Cyber Supply Chain, February 2017, p. 1.

14 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.

15 DSB, Task Force on Cyber Supply Chain, pp. 1-2.

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

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

18 NCSC, Intelligence.Gov Background Paper, p. 1.

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 U.S. adversaries, such as Russia and China, to sneak a hackable vulnerability into those systems that those nations' intelligence services can later exploit."[19] Similar concerns apply to the potential for adversaries to introduce components which are particularly vulnerable to electromagnetic threats into supply chains.

China also dominates the global capacity for IT-related assembly and manufacturing.[20] 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 equipment contracts with U.S. government and industry.[21] The U.S. also banned the use of Russian firm AO Kaspersky Lab's products from all Federal information systems, citing security concerns.[22] Adversaries can then leverage that system access for nefarious attacks.

Moreover, potential adversaries are already attempting to subvert SCRM initiatives, and can be expected to do so in the years to come. A prime example: Huawei Technologies. The Chinese ICT firm is a member in multiple cybersecurity organizations with SCRM-focused initiatives, including the Open Group (and their Open Trusted Technology Provider™ Standard (O-TTPS) Certification Program)[23] and SAFECode (and their Fundamental Practices for Secure Software Development).[24] In addition to direct supply chain threats, SCRM initiatives themselves will evidently be potential sources of adversary infiltration efforts.

19 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/.

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

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

22 Department of Homeland Security, "Notification of Issuance of Binding Operational Directive 17-01 and Establishment of Procedures for Responses," Federal Register Vol. 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.

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

24 "Members," SAFECode, n.d.a, https://safecode.org/members/.

3. Opacity and complexity of supply chains

As supply chains become more global, 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.[25]

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 difficult to vet supply chain partners beyond the first tier.[26] 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.[27] Meanwhile, adversaries can operate through multiple front companies, organizations and individuals to hide their presence, obfuscating efforts to discover and counter their actions.[28]

Given the increasing number of vendors and third-party providers on which power companies rely, "utilities often find it difficult to ensure supply chain integrity."[29] 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 information technology (IT) and operational technology (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.[30] This is creating additional vulnerabilities and increasing systems' attack surfaces. More concerning, however, is that OT system

25 NCSC, Intelligence.Gov Background Paper, p. 1.

26 National Institute of Standards and Technology, Best Practices in Cyber Supply Chain Risk Management: Vendor Selection and Management, n.d.a., 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.

27 "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.

28 Ibid., at p. 2.

29 Idaho National Library, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, August 2016, p. 15.

30 AEP, Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector, p. 4.

compromise – especially on a large scale – can have direct physical (and potentially catastrophic) consequences for infrastructure.

Options for Consideration at the Summit

- **Product vs. Vendor Certification**

  Product-by-product certification will offer the greatest potential benefits for SCRM. Given the opacity and complexity of supply chains, and the extraordinary degree to which Russia, China, and other potential adversaries can covertly penetrate them, it will be difficult to certify prime vendors rather than the specific products they sell.

- **Certification Prioritization: Initially, and long term**

  Infrastructure owners and operators typically purchase hundreds (and in many cases, thousands) of types of hardware and hardware products in a given year. The CPIC process cannot and should not certify all of these products in the early phases of the program. Instead, owners and operators should build consensus on the products that are most vital and potentially at risk – protection relays, etc. – and use that list as the starting point to launch the certification development process.

2

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 will undoubtedly be overlooked. Nevertheless, the section highlights many of the most important initiatives. They provide a basis for discussing how CPIC can support ongoing initiatives rather than replicating work, fill gaps between them, and add important new capabilities enabled by the CPIC's unique approach.

A number of important initiatives are underway to address these risks. Below are some of the most prominent, which could complement and inform the formulation of the CPIC Commission process. Many of these initiatives 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.

However, many of these initiatives also have limitations that CPIC can help address. A number of them are purely conceptual and provide no realistic or concrete basis for implementation. CPIC can provide organizations with a means to achieve such loosely-defined organizational goals. Others take implementation issues into account, but often put the burden on individual companies to perform their own threat analysis, build their own certification systems, and (magically) find sufficient providers of certified hardware and software products to meet their needs.

The CPIC initiative will centralize this process, drastically reducing duplication of resources and efforts, and providing industry-leading security at the minimum possible cost. Section III examines how CPIC can provide a more efficient and effective means of harnessing market forces and stakeholder input to strengthen supply chains on a multi-industry basis.

Nevertheless, the ongoing initiatives examined below are valuable and – in many cases – provide opportunities for partnership as CPIC moves forward. The analysis that follows examines specific contributions that these initiatives are making to supply chain resilience and identifies opportunities for CPIC to support and supplement them.

A. ENERGY SECTOR INITIATIVES

The energy sector – and particularly the electricity subsector – plays an especially 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] There are nevertheless some important initiatives underway which may form the basis of future efforts.

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 U.S. 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.

31 AEP, Identifying and Mitigating Supply Chain Risks, p. 2.

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

- **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 addresses supply chain risks in two other contexts.

- **"Research, develop and demonstrate tools and technologies to help prevent a cyber incident**

  Tools and technologies aim to decrease the cyber attack surface, protect what remains, and protect the supply chain to prevent the introduction of new vulnerabilities: …

  > *Decrease the risk posed by malicious functionality that could be inserted as components and systems traverse the supply chain. 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 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."*[35]

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."[36]

In addition, DOE's response to Executive Order 13800 – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017) provides encouraging – though 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

34 DOE, Multiyear Plan for Energy Sector Cybersecurity, p. 25.

35 DOE, Multiyear Plan for Energy Sector Cybersecurity, p. 34.

36 DOE, Multiyear Plan for Energy Sector Cybersecurity, p. 45.

cybersecurity supply chain posture and examine cyber malware impacts to components in a simulated environment."[37] It is currently unclear how much progress – if any – is underway since DOE recommended the initiative in August 2017. Nevertheless, as CPIC develops its own testing and certification scheme, it will be important for these processes to interface to reduce duplication, in a manner determined by the CPIC Commission.

The Department is also working with its national laboratories to conduct its own product testing. INL's 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."[38] DOE is also working with other national laboratories for a variety of energy sector cybersecurity-related projects through the National SCADA Test Bed.[39] 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 – 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. The CPIC Commission – particularly its representatives from the electricity subsector – should leverage this cumulative testing experience for assessing and certifying products.

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 Supply Chain Risk Management reliability standards.[40] Specifically, FERC directed NERC to develop standards which 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."[41] While they are yet to be subject to enforcement, FERC approved NERC Standards CIP-013-1 (Cyber Security

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

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

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

40 "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.

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

– 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.[42] 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."[43]

NERC's supply chain reliability standards are enormously valuable for meeting the supply chain risks in the electricity subsector. They constitute part of the foundation on which CPIC should build. However, as 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. The CPIC certification process will supplement mandatory standards by facilitating voluntary, "best in class" steps for more far-reaching supply chain resilience. The CPIC Commission should also structure the certification process to quickly account for the emergence of new threats and provide the flexibility and responsiveness necessary to meet the unanticipated supply chain challenges to come.

CPIC will supplement mandatory standards in other ways as well. 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."[44]

Moreover, 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.[45]

The CPIC initiative should be targeted to supplement and support NERC's progress. Creating a certification process that could address these systems and assets, and also benefit both BES entities and power companies not subject to the NERC standards, represents an important component of this supplemental capability.

42 Ibid. at p. 1.

43 North American Electric Reliability Corporation, CIP-013-1 – Cyber Security - Supply Chain Risk Management, July 2017, p. 3, https://www.nerc.com/pa/Stand/Project%20201603%20Cyber%20Security%20Supply%20Chain%20Managem/CIP-013-1_Clean_071117.pdf.

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

45 Ibid., at p. 3 and 8.

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 greatly 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."[46] 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 of digital computer and communication systems and networks" lays out cybersecurity requirements for complying entities.[47] 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. NRC regulatory guidance from 2010 does explicitly note the need for SCRM among their operational and management security controls. The 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).[48] NRC plans to review its cybersecurity regulations in 2019, and update as necessary.[49] As these efforts go forward, CPIC can reinforce them and provide the certification process and stakeholder-driven governance mechanisms required to help nuclear power plants meet NRC requirements to address supply chain threats. CPIC will also do so in an efficient manner by harnessing the market clout that its certification process will create for the production (and purchase) of certified hardware and software by all concerned industry sectors, worldwide.

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

47 10 CFR § 73.54 (2009), https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html.

48 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.

49 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.

Options for Consideration at the Summit

- **Strengthen a (Multi-Sector) Market for Secure Products**

  The CPIC initiative can be structured to directly meet the challenges noted by the DOE Strategy. In addition to the broad finding that "supply chain risk remains a key issue," the strategy notes that the "lack of demand" for protected products (which are likely to be of higher cost than non-secured alternatives) remains a key barrier for improving sector resilience. The multi-sector CPIC business model analyzed in section IV should directly address that barrier.

- **Multi-Sector Market**

  The CPIC initiative might initially focus on developing a certification model optimized for one or a small handful of key sectors, and then move on to other CI sectors. The energy sector could be a particularly important starting point due to the critical role the grid plays in enabling other sectors, as well as the current progress in the electricity subsector.

  The NERC standards, for example, already provide a strong foundation on which to build, especially in comparison to the weakness or total lack of equivalent standards in some other sectors. However, the fundamentals of the certification process itself are not specific to one sector or industry. The initiatives called for in the DOE strategy – many of which are already underway – could be directly incorporated into the overall CPIC development process.

  Once this initial process is well underway, including the creation of baseline certification procedures, participation by additional critical sectors would provide straightforward opportunities to expand CPIC's focus. Indeed, it is important to emphasize that the certification processes, verification mechanisms, governance, and best practices required by CPIC will be very similar across all infrastructure sectors. SCRM initiatives underway in the electricity subsector can and should be fully leveraged for use in communications, transportation, water, and other infrastructure, service, and supply sectors. Doing so will be particularly valuable given the potential for cascading failures across these increasingly interdependent sectors.

B. MULTI-SECTOR INITIATIVES

1. Department of Homeland Security (DHS)

DHS is ramping up their SCRM efforts.. DHS established its Cyber Supply Chain Risk Management (C-SCRM) program in January 18 to serve as the "lead organization and central coordination point for whole-of-government C-SCRM."[50] The initiative has an ambitious vision:

> *Enable 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.*[51]

DHS also outlined the program's major activities:

- Establish a supply chain risk assessment capability to serve stakeholders.
- Establish a communications, notification, and information sharing capability among stakeholders.
- Establish qualified bidder and manufacturer lists through implementation of 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 developing and implementing supply chain risk management capabilities.[52]

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.[53] 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."[54] Assistant Secretary for the Office of Cybersecurity and Communications at the National

50 Department of Homeland Security, Cyber Supply Chain Risk Management: Becoming a Smarter Consumer of ICT in a Connected World (slides presented at the Department of Health and Human Services' June 2018 Tech Exchange), p. 15.

51 Ibid.

52 Ibid., at p. 16.

53 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/.

54 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.

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.[55]

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."[56] Through the CDM/APL, DHS also has a specific SCRM plan, the objective of which is to "provide information to Agencies 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."[57]

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 both information technology (IT) and operational technology (OT) networks.[58] 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."[59] 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.[60] Moreover, NIST's 2017 update to their Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) includes "new details on managing cyber supply chain risks,"[61] while the April 2018

55 Jeanette Manfra, "State of Play: Federal IT in 2018," Statement for the Record Before the U.S. House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Technology, March 14, 2018, p. 8.

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

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

58 "Cyber Supply Chain Risk Management," NIST.

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

60 National Institute of Standards and Technology, Utility Sector Best Practices for Cyber Security Supply Chain Risk Management, October 2015.

61 "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.

update includes further updates on "managing cybersecurity within the supply chain."[62]

In addition to these initiatives and guidelines, NIST convenes leaders from government, the private sector, and academia to address supply chain 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."[63]

This sharing and coordination function is helpful. However, it also falls drastically short of need. It would be hugely expensive and altogether impractical to assume that individual participants in this process will 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. CPIC will supplement NIST's collaborative efforts by filling these gaps.

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 Office of Management and Budget (OMB) to oversee agency information security policies and practices. The 2016 OMB Circular A-130: Managing Information as a Strategic Resource 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.[64] 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;" and
- "[A]nalyze risks (including supply chain risks) associated with potential contractors and the products and services they provide."[65]

62 "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.

63 "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.

64 Office of Management and Budget, Circular No. A-130: Managing Information as a Strategic Resource, July 2017, p. 6, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

65 Ibid., at 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;" and
- "Develop supply chain risk management plans as described in NIST SP 800-161 to ensure the integrity, security, resilience, and quality of information systems."[66]

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 level of comprehension that CPIC intends to achieve (and indeed is necessary for truly secure supply chains). Moreover, while the policy applies to the majority of SSAs (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. Despite these faults, it is important that the CPIC Commission consider current A-130 requirements that most SSAs should already be adhering to, and potentially garner government support for CPIC by demonstrating that these Executive agencies can meet such requirements through participation in the CPIC initiative – at much lower individual organizational cost.

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."[67] They are also establishing a Vendor Risk Assessment Program (VRAP) to "evaluate known or potential risks related to suppliers of products and services."[68]

66 OMB, Circular No. A-130, p. 40 and 42.

67 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/.

68 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 (IC). 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."[69] It is supplemented by specific directives on determining the mission criticality of components, details on conducting threat assessments, and improving information sharing. While these directives apply only to the IC, CPIC can leverage best practices and apply lessons learned.

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.[70] In cooperation with DHS, NSCS also launched an industry partnership which 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 White Paper offers key SCRM findings and recommendations for both industry and government.[71] A more detailed 2017 report builds on that White Paper to provide more comprehensive recommendations – with specific regard to operational technology 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."[72]

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 AEP report's recommendations by having companies build their own certification mechanisms and create the market forces necessary to grow the supply of certified hardware and software is untenable. CPIC will facilitate supply chain resilience on a much larger and scalable basis.

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

70 NCSC, Framework for Assessing Risk.

71 AEP, Identifying and Mitigating Supply Chain Risks.

72 AEP, Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector, p. iii.

6. Department of Defense (DOD)

DOD also has an SCRM policy to achieve "trusted" systems and networks. Department of Defense Instruction (DODI) 5200.44: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks was last updated in July 2017. DODI 5200.44 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."[73] 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, though similar principals and approaches can be applied to 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 (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."[74] 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."[75]

Options for Consideration at the Summit

Taken together, these multi-sector initiatives highlight opportunities for CPIC to not only support ongoing SCRM efforts, but also fill critical gaps that remain. Particularly important: CPIC will create a centralized, industry-driven mechanism (and supporting laboratories) to certify hardware and software products, and provide a sustained validation process to stay ahead of the intensifying threat. CPIC will also supplement exigent initiatives to share emergency practices, and create the market demand necessary to incentivize and ramp up the production of secure products.

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

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

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

It will also be important to account for the policy guidance provided by Israel, the United Kingdom, and other partners in the effort. Doing so will be essential to provide for the multinational approach needed to counter the shared threat of supply chain exploitation from Russia, China, and other potential adversaries.

Supplementing the work of NIST could offer an especially useful focus for CPIC. At an industry event in February 2018, Congressman Jim Langevin noted that the adoption of the NIST Cybersecurity Framework and other risk management plans are important for reducing supply chain risk, but that "there's still room to build on those frameworks by finding consistent ways to measure the effectiveness of security controls, providing a feedback loop on the return on security investment," and improving metrics.[76] CPIC could be designed to help fill many of these gaps in ways pre-coordinated with NIST. However, while CPIC can leverage the NIST standards as part of the basis for building best practices, the initiative will ultimately be focused on delivering a more concrete, private sector-driven certification process.

C. PRIVATE SECTOR INITIATIVES

Siemens has recently joined with the Munich Security Conference and other governmental and business partners (including IBM and AES) to launch the Charter of Trust initiative. The Charter is intended to "develop and implement rules for ensuring cybersecurity throughout the networked environment."[77] As such, the effort encompasses a broad range of initiatives beyond the focus of CPIC. CPIC can also accomplish critical objectives that the Charter effort does not address. The centralized, stakeholder-driven certification process, together with the creation of industry-wide market incentives to expand the production of secure products, is especially important in this regard. The distinct priorities of the Charter and CPIC could nevertheless provide valuable opportunities for mutual support.

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] Unlike Principle 7, however, CPIC will provide value as a

76 Heckman, "DHS, lawmakers doubling down on supply chain risk management," Federal News Radio.

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, Charter of Trust: For a secure digital world, February 2018, https://www.siemens.com/press/pool/de/feature/2018/corporate/2018-02-cybersecurity/charter-of-trust-e.pdf.

non-mandatory initiative, avoiding burdensome regulatory compliance certification efforts. As a voluntary scheme, CPIC can also offer added value by operating on best practices – beyond the often minimally sufficient baseline of mandatory standards.

Options for Consideration at the Summit

components, the company is especially well-positioned for coordination with the development of the certification mechanisms envisioned for CPIC. The Charter of Trust effort also includes companies in an array of infrastructure sectors, including transportation, which will be essential for Black Sky preparedness. Summit participants should consider how best to explore coordination opportunities with Charter participants, who will be similarly determined to secure critical supply chains. Indeed, Principle 7 of the Charter's requirement for "independent third-party certifications" for infrastructure components appears to call for exactly the type of body CPIC aims to become.

3

PRODUCT CERTIFICATION

To be effective as a certification commission, CPIC will also need to leverage progress and lessons learned from ongoing efforts in product certification. This section specifically examines product certification schemes to serve as a potential starting point for the CPIC Commission – which, if it is to provide actionable, operational mitigations for SCRM, will need to be a certification body. Organizations and initiatives exist, largely in the private sector, to assess potential risks to specific products, processes, and systems. There are a great number of these organizations worldwide, though only a few are surveyed here. An increasing number of these certification bodies are including considerations for cybersecurity. Few certify for electromagnetic thresholds.

These certifying organizations typically lack key features of the proposed stakeholder-driven process that will make CPIC so effective. However, they do offer models that can be used as CPIC develops its own certification process. Some of these organizations may also become valuable partners for CPIC, especially as the initiative focuses on activities that fill gaps in existing certification efforts.

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] UL is an industry leader in the U.S., and working with manufacturers, industry experts, other testing labs, and governments, UL testing standards often become the "de facto standards of the US government."[80] UL can also serve as an independent third party to certify

79 "Certification," Underwriters Laboratories, n.d.a., 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 U.S. Department of Labor's Occupational Safety and Health Administration considers UL as one of its Nationally Recognized Testing Laboratories.[82]

Given their history, it may be tempting to simply task UL (or a similar company) to undertake a CPIC-like effort themselves. Such an organization would surely have much of the expertise required to develop the CPIC initiative. However, considering their current organizational structure and commitments, certification bodies such as UL alone would not likely be able to sufficiently mobilize or focus resources to develop CPIC with the expediency required to address the threat. Moreover, the CPIC Commission will ideally provide additional value added by bringing together leaders from a broad range of sectors, giving the initiative inherent connectivity to each industry's unique resilience requirements.

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 information technology.[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 and possible application to CPIC certification efforts. 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]

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

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

83 "ISO/IEC JTC 1 — Information Technology," International Organization for Standardization, n.d.a., 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 http://isa99.isa.org/Public/Information/The-62443-Series-Overview.pdf

The ISO/IEC standards can help inform the criteria that the CPIC Commission will use in its own certification scheme. However, these standards are no substitute for the CPIC initiative's much more comprehensive vision. Further outreach will be necessary to determine the extent to which (and how) ISO/IEC provides continuing testing and verification of products and vendors. Nevertheless, in addition to such a scheme, the CPIC initiative will provide additional benefit by maintaining connectivity to a range of sectors and stakeholders required to expand and incentivize participation in the process.

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 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]

The CPIC Commission should consider analyzing the SAFETY Act as a possible model for standard-setting and governance. One area of interest: the SAFETY Act certification lasts for a term of five to eight years, and vendors may apply for renewal at any point within two years prior to the expiration.[92] While cyber threats will likely necessitate a smaller window for re-evaluation, and the CPIC will likely require a more narrow focus than the SAFETY Act currently employs, the Commission can assess the

87 "Research and Development Partnerships – SAFETY Act for Liability Protection," Department of Homeland Security, January 14, 2014, https://www.dhs.gov/sites/default/files/publications/Safety%20Act%20for%20Liability%20Protection_0.pdf.

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

89 "Research and Development Partnerships – SAFETY Act for Liability Protection," Department of Homeland Security, January 14, 2014, https://www.dhs.gov/sites/default/files/publications/Safety%20Act%20for%20Liability%20Protection_0.pdf.

90 Ibid.

91 Ibid.

92 6 CFR § 25.6, Section (f), https://www.law.cornell.edu/cfr/text/6/25.6.

potential applicability of SAFETY Act processes and procedures for certification and renewal.

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 information technology products has existed for over 30 years.[93] 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 and cost-effectiveness of the evaluation and certification/validation process."[94] CC has certified 2,351 products as of June 5, 2018, which include access control devices and systems, operating systems, detection devices and systems, boundary protection devices and systems, etc.[95]

Given the CC's mission statement and goals, they constitute an ideal partner for CPIC. As with many cybersecurity-focused (rather specifically than infrastructure-focused) initiatives, one potential flaw lies in CC's focus on IT rather than OT. However, that presents an opportunity for CPIC to provide added value. In addition, its membership does not include any participation from China, Russia, or any other near-peer cyber adversaries.[96] 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."[97]

A range of other public and private sector cybersecurity certification programs exist, and CPIC members should collectively decide which may constitute potential partners – and which to avoid. 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.

93 Steven B. Lipner, SAFECode Perspective on Cybersecurity Certification, January 2018, p. 1.

94 "About the Common Criteria," Common Criteria, n.d.a, https://www.commoncriteriaportal.org/ccra/index.cfm.

95 "Certified Products," Common Criteria, n.d.a., https://www.commoncriteriaportal.org/products/.

96 "Members of the CCRA," Common Criteria, n.d.a., https://www.commoncriteriaportal.org/ccra/members/.

97 "About the Common Criteria," Common Criteria, n.d.a, https://www.commoncriteriaportal.org/ccra/index.cfm.

Nevertheless, both organizations' functions are similar to what is envisioned for CPIC and would have otherwise been ideal partners for the CPIC Commission's development stages.

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."[98] Notably, SAFECode is helping the small and mid-sized organizations which are struggling to keep up with major organizations worldwide that have funded their own SCRM programs.[99] As it will be examined in Section IV, 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 that could supplement – or already align with – current CPIC thinking. 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.[100] 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."[101] 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."[102]

While SAFECode is all but ruled out as a CPIC partner due to its membership, this report also notes that their initiative is also insufficient for infrastructure SCRM due to its sole focus on IT (rather than OT) products. Unlike CPIC, SAFECode also appears to place the onus for compliance, testing, and verification on organizations themselves. SAFECode's Fundamental Practices for Secure Software Development can nevertheless provide CPIC Commission members with an additional source of insights as they develop the certification program.[103]

98 Steven B. Lipner, SAFECode Perspective on Cybersecurity Certification, January 2018, p. 2.

99 Ibid., at p. 3.

100 Ibid., at p. 2.

101 Ibid.

102 bid.

103 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

b. O-TTPS Certification Program

The Open Group O-TTPS program also aligns with the envisioned CPIC initiative The 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."[104] The Open Group certifies organizations that they deem to comply with the program requirements as "Open Trusted Technology Providers™."[105]

O-TTPS policy and guidance documents can also provide important foundational material for the CPIC initiative development. The 2017 certification policy document, for example, includes detailed workflow diagrams for third-party certification, with additional detail for each step of the process.[106] The document also includes specific policies for conformance requirements, maintaining certification, re-certification, and an appeal process for certification decisions, among others.

104 "The Open Trusted Technology Provider™ Standard (O-TTPS) Certification Program," The Open Group, n.d.a, http://www.opengroup.org/certifications/o-ttps.

105 Ibid.

106 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.

4

BUILDING A BUSINESS MODEL FOR CPIC

Very little international collaboration exists to address supply chain risks which incorporate all relevant stakeholders (although the Charter of Trust initiative takes preliminary steps in that regard). Multi-sector collaboration in the U.S. alone has barely begun. Moreover, the initiatives listed above vary in their level of detail and tangibility. While some provide very specific requirements or standards, few include comprehensive processes to implement these standards through ongoing validation efforts and capabilities. Others merely draw attention to the importance of supply chain threats and associated risk management efforts without providing guidance on how to implement such measures.

This call to attention is important. However, in addition to a multi-sector awareness campaign, CPIC can help organizations and government agencies already aware of cyber supply chain threats implement risk management initiatives that will meaningfully bolster infrastructure cybersecurity.

To meet these goals, however, it will first be necessary to develop a model for advancing the CPIC initiative that is politically and economically viable. While government procurement requirements are essential for helping government agencies and Defense Industrial Base companies defeat attacks on their supply chains, government mandates alone cannot meet the needs of infrastructure owners and operators. Instead, CPIC should establish a voluntary, "demand-driven" business model to incentivize vendors to secure selected segments of their hardware and software product portfolios against corruption.

Infrastructure owners and operators and product and service suppliers are increasingly focused on buying products that are malware-free. Through the CPIC initiative, industry leaders from multiple sectors can work collectively to develop and optimize a product certification process that leverages the financial incentives offered by an expanding, multi-sector user group to foster the availability and broad use of secure product lines.

Doing so in coordination with U.S. and allied government agencies will ensure even broader applicability and strengthen the demand signal for secure products. By purchasing products that meet those standards, owners and operators can help bolster the emerging standards and market forces essential to improve SCRM.

This section examines opportunities for CPIC to provide unique value by filling gaps and shortfalls in current initiatives. The section also offers preliminary options for Summit participants to discuss and consider for developing such an incentives-based ecosystem.

Preliminary Options and Issues for Consideration by CPIC Summit Participants

1. Leveraging existing company plans and capabilities for SCRM

Many private sector entities, including grid owners and operators participating in the Summit, 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, at least 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.

A key goal for the Summit should be to begin to identify and capture these best practices. Participants should also discuss how existing re-certifications (i.e., DHS' CDM program) or vendor risk assessments (i.e., GSA's VRAP) might also be useful in the CPIC development process.

2. Centralized coordination

Many industry and government best practices nevertheless face a similar shortfall that CPIC can help address. One of the foremost advantages of CPIC's business model relative to current approaches is the initiative's centralizing function. 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. Indeed, if CPIC can incentivize participation by most sectors in the U.S. and allied nations, and secure procurement funding commitments from these partners, the initiative could leverage the resources available to build best in class standards and certification processes. In turn, these partners will ideally be motivated to meet such standards and use the CPIC-certified products.

3. Guarding against "minimalist" standards

While 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.[107] 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."[108]

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 is not intended to 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 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 re-evaluation 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 as well). However, the United Kingdom, Israel and the other nations represented at the Summit also have cutting-edge SCRM initiatives underway.

The Summit provides a unique opportunity to share differing national models to help launch the CPIC development process. It also provides an opportunity to develop –

107 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.

108 AEP, Identifying and Mitigating Supply Chain Risks, p. 2.

from the beginning –a certification process that will be applied to the full, international footprint of modern technology product supply chains.

Internationalizing the CPIC effort can also help create and expand the necessary customer and product user base. Supply chain exploitation efforts by Russia, China, and other nations are multi-sector and global in nature. The CPIC initiative should be structured accordingly. This internationalized approach will also need to retain CPIC's focus on certifying hardware and software products that are most vital to prevent large scale failures in critical sectors and reinforce Black Sky resilience.

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.

Participants could also consider adding a middle tier that approaches best in class ("Prime") but provides some leeway on the most institutionally, politically, or operationally challenging requirements. Such a tiered system could also benefit regulators who may wish to tie regulatory requirements to CPIC certification – and would likely use the basic rather than prime standard.

6. Role of government

Senior government officials from all participating countries need to play a key role in the CPIC development process to make the initiative successful. 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.

7. Draft Charter

The CPIC™ Commission Initiative Inaugural Summit Meeting, taking place on June 27 as part of EIS Summit IX in London, is designed as the first event in a three meeting, 12-month series. The meeting should lead to a draft CPIC Initiative charter. The charter should be formulated to define the bones of the envisioned commission, which will grow over time to address both a wider range of products and associated sectors, and more extensive validation capabilities. The charter itself should include fundamental guiding principles, membership and member categories, the makeup of the governing and advisory bodies, the scope and timeline of the initiative, international cooperation mechanisms, and more.

By facilitating voluntary collaboration among owners and operators of infrastructure sectors, along with their government partners, CPIC can provide a unique opportunity for private and public sector leaders in the United States, Israel, the United Kingdom and organizations in other participating nations to address one of the most serious, growing risks faced by modern society.


EIS
COUNCIL