CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT TASK FORCE: INTERIM REPORT

Status Update on Activities and Objectives of the Task Force

September 2019

This page is intentionally left blank.

FOREWORD

We are pleased to share this Interim Report (Report) describing the work of the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)'s Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force (Task Force) over the past year.

As the Sector Specific Agency for the Communications and Information Technology Sectors, DHS serves as a focal point and convener for a broad national community of ICT stakeholders.[1] This community includes representatives from all federal civilian agencies, critical infrastructure owners and operators, and state, local, tribal, and territorial (SLTT) governments. It coordinates with the other parts of the Federal Government. Together, the ICT stakeholder community provides expertise and recommendations necessary to secure the Nation's ICT infrastructure from all hazards, a fundamental priority for homeland and national security.

The Task Force was formed in 2018 with strategic mandates to provide a forum for the collaboration of private sector owners and operators of ICT critical infrastructure and to provide advice and recommendations to DHS on means for assessing and managing risks associated with the ICT supply chain. Chartered under the National Infrastructure Protection Plan Framework and the associated Critical Infrastructure Partnership Advisory Council (CIPAC), the Task Force's efforts are directed by a collaborative leadership team with representatives from DHS and the Communications and Information Technology Sectors. The Task Force's constituent Working Groups are comprised of sector members, subject matter experts from those sectors, and representatives from across the Federal Government.

This Report describes the structure and mission of the Task Force and its four constituent Working Groups, detailing the operating models, primary areas of discussion, and, where appropriate, key findings of each. This work lays an important foundation for the Task Force as it enters its second year of effort. Thus, this Report also recommends strategic priorities and direction for future Task Force efforts, informed by statutory and policy mandates.

We look forward to continued collaboration. Within DHS, CISA will maintain engagement with the ICT stakeholder community to assure that the path forward leverages industry's and government's collective expertise to meet the fundamental challenge of securing the ICT supply chain, an important homeland and national security priority.

On behalf of ourselves and the Department's leadership, we wish to express appreciation for the investment of time and resources made by Working Group and other Task Force participants.

Bob Kolasky
Assistant Director, CISA
National Risk Management Center

Robert L. Mayer

Robert Mayer
Senior Vice President
US Telecom
Communications SCC Chair

Vice President of Policy
ITIC
IT SCC Chair

[1] The White House, "Presidential Policy Directive 21 (PPD-21) - Critical Infrastructure Security and Resilience," February 2013.

EXECUTIVE SUMMARY

U.S. critical infrastructure and governments at all levels rely heavily on Information and Communications Technology (ICT). Ensuring resilience and trust in our ICT supply chain is more than just a cybersecurity issue – it touches national security, economic security, and public health and safety.

Effective supply chain risk management is a national imperative. This effort will require a whole of government and whole of society approach. Continued technological advancement in the ICT supply chain – with welcomed developments in 5th Generation (5G) mobile communications – only increases the necessity to take this issue seriously.

This Interim Report (Report) describes the work of the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)'s Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force (Task Force) over the past year. As described in this Report, the Task Force is a collaborative endeavor between representatives of industry and government designed to investigate and recommend methods to manage ICT supply chain risks. Its agile, mission-focused approach addresses these issues head-on and provides actionable outputs that create tangible results.

Task Force leaders come from DHS and the Communications and Information Technology sectors. Task Force members include members of both sectors, as well as representatives from across the Federal Government.

The Task Force's combination of industry and governmental expertise has yielded strong results in its first year. This Report details the Task Force's methodologies, areas of discussion, and, where appropriate, key findings, recommendations, and potential areas for further study identified by each of the Task Force's four constituent Working Groups (WG), highlighting impacts of the Task Force's overall mission on supply chain risk management. Each Working Group addressed an area of significant policy concern in addressing SCRM challenges, including:

- The timely sharing of actionable information about supply chain risks across the community (WG1);
- The understanding and evaluation of supply chain threats (WG2);
- The identification of criteria, processes and structures for establishing Qualified Bidder Lists (QBL) and Qualified Manufacturer Lists (QML) (WG3); and
- Policy recommendations for incentivizing the purchase of ICT from original equipment manufacturers and authorized resellers only (WG4).

The findings and recommendations of the Working Groups from this past year will be foundational to the Task Force's second year of activity. In its next phase, the Task Force and the Working Groups will continue to support efforts by the Federal Government and industry to manage ICT supply chain risk.

PARTICIPATING ORGANIZATIONS

The voting membership of the Task Force was drawn from throughout the supply chain risk management ecosystem. Members represented a range of government and industry stakeholders, ensuring the Task Force would be able to effectively consider inputs from across the public and private sectors. The following table lists the participating organizations of Task Force members.

TABLE 1—PARTICIPATING ORGANIZATIONS OF ICT SCRM TASK FORCE MEMBERS

USG PARTICIPATING ORGANIZATIONS	IT SECTOR PARTICIPATING ORGANIZATIONS	COMMUNICATIONS SECTOR PARTICIPATING ORGANIZATIONS
Federal Bureau of Investigation	Accenture	AT&T
Federal Communications Commission	BSA	CenturyLink
General Services Administration	Cisco Systems	Charter Communications
National Aeronautics and Space Administration	Coalition for Cybersecurity Policy & Law	Comcast
National Institute of Standards and Technology	CyberRx	CompTIA
Nuclear Regulatory Commission	Cyxtera	Cox
National Security Agency	Dell	CTIA
National Telecommunications and Information Administration (NTIA)	FireEye	Iconectiv
Office of the Comptroller of the Currency	General Dynamics Information Technology	National Association of Broadcasters
Office of the Director of National Intelligence	HP	NCTA
Social Security Administration	IBM	NTCA – The Rural Broadband Association
U.S. Department of Commerce	Information Technology – Information Sharing Analysis Center	NTT
U.S. Department of Defense	Information Technology Industry Council	Pioneer
U.S. Department of Energy	Intel	Sprint
U.S. Department of Homeland Security	Interos Solutions	T-Mobile
U.S. Department of Justice	Microsoft	USTelecom
U.S. Department of the Treasury	Palo Alto Networks	Verizon
	Samsung	
	Synopsys	
	Threat Sketch	

Additionally, individuals from the following organizations provided support or participation to the Task Force, including invaluable participation from representative members in leading and contributing to Working Group efforts within the Task Force. Contributors and participants in the Task Force included representatives from the Office of Management and Budget (OMB), Blue Valley Telecommunications, CDW-G, Cert, E.W. Scripps Company, Ericsson, Farmers Telecommunications Cooperative (Alabama; NTCA Member), Hodgkins Consulting, LLC, Hubbard Broadcasting, Juniper Networks, NTT, Quincy Media, Rehancement Group, Safecode, Tenable, and Venable, LLP.

Contents

SECTION I — INTRODUCTION

U.S. critical infrastructure and governments at all levels rely heavily on ICT. Ensuring resilience and trust in the ICT supply chain is more than just a cybersecurity issue – it is an issue that impacts national security, economic security, and public health and safety.

The Design, Development and Production, Distribution, Acquisition and Deployment, Maintenance, and Disposal phases of the ICT supply chain are susceptible to the deliberate or inadvertent introduction of vulnerabilities. Malicious software and hardware; counterfeit components; and poor product designs, manufacturing processes, and maintenance procedures all threaten the resilience of the ICT supply chain.

These risks are not theoretical. In recent years malicious actors have successfully: hijacked cellular devices, infected switch flash cards, pre-installed malware on end user devices, sold counterfeit ICT to U.S. armed forces, and embedded malware within software security tools.

Effective management of ICT supply chain risks is a national imperative. The scale of this challenge requires a whole of government and whole of society approach. Continued technological advancement within the ICT supply chain, with welcome developments in 5G mobile communications, further necessitates the need to address this challenge with greater urgency and action.

In late 2018, DHS CISA, in partnership with Communications and Information Technology sectors, took the important step of establishing the ICT SCRM Task Force. The Task Force acts a convening body for public and private sector ICT experts, focusing broad efforts into specific initiatives that tackle ICT supply chain risks head-on. The Task Force was chartered to convene private sector owners and operators of ICT critical infrastructure and provide advice and recommendations about assessing and managing risk in the ICT supply chain to DHS.

As the Task Force enters its second year of operations, this Report describes the progress made over the past year and outlines potential future directions of Task Force efforts. In summarizing first year work products and associated impacts, the Report describes the Task Force's convening role within the context of the broader ICT SCRM ecosystem.

The Task Force has acted as a fulcrum, concentrating the efforts of government and private industry on building a collaborative framework.

In detailing the progress made and future directions, this Report is broken into the following sections:

- Section II consists of an overview of the Task Force, its structure, and its organizational objectives;
- Section III provides an overview of the broader ICT environment, ongoing supply chain efforts, and cross-sector collaborative approaches, including an inventory of SCRM standards and best practices;
- Sections IV-VII review the structure, processes, findings and initial recommendations from the Task Force's four Working Groups; and
- Section VIII outlines the Task Force's future direction, based on its first-year findings and proposed recommendations for future consideration.

This Report has been developed with multiple audiences in mind. Its findings and recommendations are relevant to the ICT stakeholder community, as well as a broader group of stakeholders, including members of the Federal Acquisition Security Council (FASC) (the Council's agencies are all represented on the Task Force), the U.S. Congress, additional components of the Federal Government and state, local, tribal, and territorial (SLTT) governments, and critical infrastructure owners and operators.

This Report is an informational document. While it includes updates on the Task Force's progress and recommended future direction, it does not constitute policy decisions or a definitive plan for the future efforts of the Task Force, CISA, DHS, or the U.S. Government.

SECTION II — TASK FORCE OVERVIEW

The ICT SCRM Task Force is a forum for collaboration between representative experts from both the public and private sectors. The Task Force organization enables government and industry experts to work together on an ongoing basis and leverage the results of past efforts[2] and existing knowledge to create actionable recommendations. These recommendations inform strategic, policy, and operational decision-making pertaining to the identification, prioritization, and mitigation of ICT supply chain risks.

2.1 Purpose

The Task Force was chartered in late 2018 with the express purpose of advising the government and private sector critical infrastructure owners and operators on means for assessing and managing risks associated with the ICT supply chain.[3] Thus, the Task Force is an essential part of broader DHS efforts promote ICT security and resilience, as part of its larger critical infrastructure protection mission. Chartered as a consensus-based body under the Critical Infrastructure Partnership Advisory Council (CIPAC), the objectives of the Task Force are:

- To act as a forum for collaboration with private sector owners and operators of critical infrastructure, through their respective Sector Coordinating Councils (SCC), on methods and practices to effectively identify, prioritize, and mitigate ICT supply chain risks;
- To provide realistic, actionable, timely, economically feasible, scalable, and risk-based recommendations for addressing ICT supply chain risks; and
- To recommend methods for the development and implementation of initiatives, including mutually beneficial private-public-partnerships, designed to improve risk management in global ICT supply chains.

The Task Force is an embodiment of DHS's collective defense approach to cybersecurity risk management, as encapsulated in the work of CISA's National Risk Management Center, which stewards the Task Force.

2.2 Task Force Membership

The Task Force is a public-private collaboration that includes 60 members from federal agencies, the Communications Sector Coordinating Council (Communications SCC), and the Information Technologies Sector Coordinating Council (IT SCC). Forty representatives from private sector organizations from the IT and Communications sectors contribute to the Task Force and are joined by a further 20 representatives from the Federal Government. The Task Force is led by three Co-Chairs: Robert Mayer (Chairman, CSCC) represents the Communications Sector, John Miller (Chairman (IT-SCC) represents the IT Sector, and Bob Kolasky (CISA Assistant Director, National Risk Management Center) represents government members.

Members are able to leverage the assistance and expertise of colleagues from their organizations to support Task Force efforts, as appropriate. Additionally, ICT subject matter experts from organizations not represented by the membership are included in working group activities, upon approval of the Task Force leadership.

In addition to the members, the Task Force received invaluable contributions, expertise, and participation from a range of stakeholders from across the public and private sectors. The Task Force membership offers a diverse group, with members and other participants representing a wide array of organizations and serving in a variety of roles. This design allows members to bring diverse perspectives from both large and small organizations with roles in shaping supply chain risk management practices. Ultimately, the objective of this

[2] CNCI 11 (2010 Report); DoD Trusted Systems & Networks Working Group; NIST/DoD/GSA/DHS Software & Supply Chain Assurance Forum; NTIA Software Assurance Working Group.
[3] Charter for the Information and Communications Technology Supply Chain Risk Management Task Force, revised 12/13/2018.

type of public-private partnership is to share recommendations and guidance proposed by the Task Force with both industry and government stakeholders. Such a partnership helps to guide all producers and consumers of ICT, both government and industry alike, on methods to enhance their cyber supply chain risk management. The list of participating organizations can be found in Table 1.

2.3 Task Force Lines of Effort

The Task Force utilizes the National Infrastructure Protection Plan (NIPP) Framework, including the Critical Infrastructure Partnership Advisory Council (CIPAC) structure, to facilitate effective information exchange between government, industry partners, and subject matter experts. This structure provides a flexible methodology to engage parties to solve critical problems.

To better accomplish the Task Force priorities set forth in initial planning and strategy sessions, four constituent Working Groups were established, comprising industry and governmental expertise in specific domains. Each of the four Working Groups established in the first phase of the Task Force addressed a specific issue area:

- **Working Group #1: Information Sharing** – Development of a common framework for the bi-directional sharing of actionable supply chain risk information across the community.
- **Working Group #2: Threat Evaluation** – Identification of processes and criteria to better understand and evaluate threats to ICT supplies, products, and services.
- **Working Group #3: Qualified Bidder Lists and Qualified Manufacturer Lists (QBL/QML)** – Identification of market segments and evaluation criteria to establish Qualified Bidder and Qualified Manufacturer Lists that address considerations of vendor and product inclusion and exclusion.
- **Working Group #4: Policy Recommendations to Incentivize Purchase of ICT from Original Equipment Manufacturers (OEM) & Authorized Resellers** – Policy recommendations principally aimed at stopping the growing problem of counterfeit ICT procurement.

The Task Force selected these Working Groups through a process that provided transparency, traceability, and the ability to inform future Working Group selection efforts. Initial topics were identified to align to priorities set forth by the Co-Chairs or otherwise identified from relevant guidance. The Task Force combined these topics with those put forth by Task Force members, other government officials, and other stakeholders in the critical infrastructure community. Task Force members then voted on potential Working Group topics through a survey. The four topics selected garnered significantly more support than the other proposed topics.

The Task Force and the respective Working Groups recognized the unique circumstances and needs of small and medium-sized businesses. These factors were part of considerations across the Task Force and the Working Groups, with a focus on ensuring that outputs and their efforts would work to address these challenges. The Task Force strives to provide holistic recommendations that ensure applicability for small and medium-sized businesses and provide actionable steps for these stakeholders to incorporate inputs, products, and recommendations.

2.3.1 CATALOGUING EXISTING SUPPLY CHAIN RISK MANAGEMENT SUPPORT

In addition to the four selected Working Groups, Task Force members agreed to develop an inventory of supply chain risk management efforts within government and industry. A wide range of critical infrastructure stakeholders have expressed concern that the totality of supply chain risk management activity is difficult to effectively monitor due to its scale. The resulting inventory clarifies the supply chain risk management landscape.

2.4 Connections to Other Federal Supply Chain Activities

The Task Force's efforts have advanced interagency supply chain risk management priorities. For example, it has, and continues to, coordinate with the FASC to help ensure the effectiveness of implementation of the *Federal Acquisition Supply Chain Security Act.* Additionally, NSC and OMB representatives frequently attend Task Force meetings to maintain situational awareness of Task Force activities.

Task Force members also provided private sector input into the DHS-led ICT criticality assessment, pursuant to Executive Order 13873. This input has resulted in the segmentation of the ICT supply chain into five roles, eleven sub-roles, and 61 elements (ICT hardware, software, and services). DHS has stated that it hopes this segmentation will provide a helpful, standardized taxonomy when discussing ICT criticality during the next phase of the Task Force's efforts. It also provides guidance to shape discussions relating to ICT efforts within the broader supply chain ecosystem. Additional information can be found here: https://www.cisa.gov/cisa/supply-chain-risk-management.

SECTION III — ICT SUPPLY CHAIN RISK MANAGEMENT OPERATING ENVIRONMENT

3.1 The ICT SCRM Task Force and ICT Supply Chain Risk

ICT is one of the largest areas of economic activity on the planet. Market estimates of annual expenditures highlight the economic impact of commercial off the shelf (COTS) ICT hardware and software products and services. $500 billion of the annual investment in ICT comes from the U.S. Government's and critical infrastructure owners' and operators' ICT activities.[4]

As this market continues to grow, so does the risk to the ICT supply chain and its ever-expanding user base. A 2018 Symantec report detailed that the number of observed supply chain attacks was 78 percent higher in 2018 than it was in 2017, as malicious actors sought to exploit vulnerabilities in third-party software, hardware, and services.[5] A 2018 National Counterintelligence and Security Center Report "Foreign Economic Espionage in Cyberspace" characterized 2018 as a "watershed year in software supply chain reporting."[6] Recognizing a "catastrophic" impact stemming from sustained ICT supply chain threats, in May 2019, President Trump signed an Executive Order authorizing the Commerce Secretary to regulate acquisition and use of information and communications technology and services from foreign adversaries.[7]

The size of the economic value of the U.S. Government's share of purchases of ICT makes government a critical stakeholder. However, in combination with the purchases of the Nation's critical infrastructure providers, owners and operators of critical infrastructure bear a large portion of the impact of failures of supply chain hygiene. Therefore, the U.S. Government has an undeniable interest in partnership with industry and in furthering its role as steward of taxpayer dollars. It has an interest in identifying and remedying abuses of the ICT supply chain which could impact the availability, confidentiality, and integrity of critical infrastructure.

New sources and tools to identify and raise awareness of supply chain risks and new legal authorities from Congress have led to a range of nascent activities across both vendor industries and their government customers to address SCRM threats. Armed with new legal authorities, DHS and its government partners can address supply chain risk both through the role as ICT customers and through their responsibilities for critical infrastructure protection for the Nation's most vital infrastructure sectors. DHS and its partners are today working collaboratively to address supply chain abuses and threats that may impact critical infrastructure such as financial services, health care, manufacturing, transportation, and ICT itself, as well as millions of small businesses and individual technology users themselves.

This partnership provides a significant opportunity for progress by leveraging the technical expertise of ICT vendors to address an issue that is understood as a shared responsibility.

[4] Gartner; Frost & Sullivan market estimates: DoD/IC classified, $100 b. DoD MilSpec embedded ICT $50 billion DoD (U) COTS ICT $100 billion WoG Civilian ICT $100 billion SCMLT COTS ICT $100 b. Critical Infrastructures $50 b. Gartner Global ICT Market Estimate. https://www.gartner.com/en/webinars/3894565/it-spending-forecast-4q18-update-what-will-make-headlines-in-201.

[5] *SecurityWeek*. Arghire, Inout. "Supply Chain Attacks Nearly Doubled in 2018: Symantec." Feb. 20, 2019. Accessed Sept. 6, 2019. https://www.securityweek.com/supply-chain-attacks-nearly-doubled-2018-symantec.

[6] National Counterterrorism and Security Center. Foreign Economic Espionage in Cyberspace. https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

[7] Executive Order on Securing the Information and Communications Technology and Services Supply Chain. May 15, 2019. https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

3.2 Industry Standards Inventory Effort

The Task Force has also assessed the standards and practice environment. This included the development of an inventory of applicable standards developed by voluntary industry standards bodies and government processes, including those mandated by law. The inventory additionally reviewed other critical practice guidance elements of the ICT environment and relevant laws and policies.

The inventory identified the standards organization, the SCRM standard or guidance, and descriptive information materials, where publicly available. Aggregating this information helps to lay the foundation for assessing the utility and utilization methods for development of SCRM programs, applicability of specific use cases, and identification of gaps and improvements in SCRM methods.

During inventory development, Working Group members associated standards with the logical "threat groups" provided by Working Group 2 to aid in identifying the applicability of specific standards. These threat groups are as follows and correspond to the identified items in the inventory:

A. Counterfeit parts

B. Cybersecurity

C. Internal Security Operations and Controls

D. System Development Life Cycle (SDLC) Processes and Tools

E. Insider threats

F. Economic risks

G. Inherited Risk (Extended supplier chain)

H. Legal risks

I. External end-to-end supply chain risks (natural disasters, geo-political issues)

A detailed "Inventory of Supply Chain-related Standards" and a brief summary index provides descriptive information and links to the underlying publications. The Inventory and index table can be used by the broader ICT Supply Chain community as a foundation for assessing applicability of standards to specific use cases and to identify gaps and potential improvements in SCRM methods.

TABLE 2—SUMMARY INDEX: INVENTORY OF SUPPLY CHAIN-RELATED STANDARDS & BEST PRACTICES

NUMBER	BODY, STANDARD	FUNCTION	THREAT GROUP
1	International Organization for Standardization (ISO) ISO/IEC 27001: Information Security Management-Requirements (10/01/2013)	Best practice exemplifies information security maturity of an organization; demonstrates good cyber hygiene	C
2	Center for Internet Security (CIS) Critical Security Controls for Effective Cyber Defense Control 4: Continuous Vulnerability Assessment and Remediation (Version 6, 2015)	Key controls for essential cyber defense readiness	C
3	Information Systems Audit and Control Association (ISACA) COBIT 5 / ISACA (V.5, 2012) • AP010 "Manage Suppliers" • AP012 "Manage Risk"	Standards that support balance between realizing benefits and optimizing risk levels and resource use	C

NUMBER	BODY, STANDARD	FUNCTION	THREAT GROUP
	• AP013 "Manage Security" • BAI01 "Manage Programmes and Projects" BAI02 "Manage Requirements Definition"		
4	International Society of Automation (ISA)ANSI/ISA–62443-2-1 (99.02.01)–2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program	Minimum requirements to achieve cyber security for industrial systems	C
5	National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations, (SP 800-53, Rev. 4) (2013; Rev. 5 pending)	Comprehensive set of security controls for federal agencies, including more than 20 expressly addressing SCRM, and guidance to tailor baseline to meet mission and environmental factors	C
6	National Institute of Standards and Technology (NIST) Guide for Conducting Risk Assessments. SP (Special Publication) 800-30, Rev. 1 (2012)	Technical procedures for risk assessment for non-National Security IT systems at federal agencies and state/ local government	C
7	International Organization for Standardization, Specification for Security Management Systems for the Supply Chain: ISO/IEC 28000 (2007/2011)	Specifies the requirements for a security management system, including aspects critical to security assurance of the supply chain	C
8	International Organization for Standardization (ISO) Risk management - Risk assessment techniques: ISO/IEC 31010 (2009)	Supports ISO 31000. Provides a generic/high level risk management standard	C
9	International Organization for Standardization (ISO) Freight Containers - Mechanical Seals: ISO/IEC 17712 (May 2013)	Addresses physical risk to extended supplier chain by setting forth a single source of information relating to seals used to secure freight containers	G
10	International Organization for Standardization (ISO) Mitigating Maliciously Tainted and Counterfeit Products -- Part 1: Requirements and Recommendations: ISO/IEC 20243-1:2018 (2018)	Set of guidelines, requirements, and recommendations that address threats from maliciously tainted and counterfeit COTS ICT hardware and software throughout the product life cycle	I
11	The Open Group Open Trusted Technology Provider Standard Certification Program O-TTPS (2014)	Certification program relating to conforming to standards for product integrity coupled with supply chain security	C
12	International Organization for Standardization (ISO) Information Security for Supplier	Guidance to assist organizations in securing data and information	B

NUMBER	BODY, STANDARD	FUNCTION	THREAT GROUP
	Relationships Security Techniques-Part 1: Overview And Concepts ISO/IEC 27036-1:2014 (2014)	systems within the context of supplier relationships	
13	International Organization for Standardization (ISO) Information Security for Supplier Relationships Security Techniques-Part 2: Requirements ISO/IEC 27036-1:2014 (2014)	Specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships	B
14	International Organization for Standardization (ISO) Information Security for Supplier Relationships Security Techniques-Part 3. Guidelines for information and communication technology supply chain security ISO/IEC 27036-3:2013 (2013)	Guidance on gaining visibility into the information security risks associated with physically dispersed and multi-layered global ICT supply chains	B
15	International Organization for Standardization (ISO) Information Security for Supplier Relationships Security Techniques-Part 4. Cloud Services ISO/IEC 27036-4:2016 (2016)	Guidance on gaining visibility into the information security risks associated with the use of cloud services and managing those risks effectively and responding to user risks specific to the acquisition or provision of cloud services that can have an information security impact	B
16	International Electrotechnical Commission Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements: IEC 62443-4-1:2018 (2018)	Defines requirements for the secure life-cycle development of process automation and industrial control systems that can be specified for use by designer or maintainer of a product	D
17	International Organization for Standardization (ISO) ISO 19678 (NIST SP 800-147): BIOS Protection Guidelines ISO 19678 (2015)	Provides requirements and guidelines for preventing the unauthorized modification of Basic Input/Output System (BIOS) firmware on PC client systems	B
18	International Organization for Standardization (ISO) ISO 9001 Quality Management System (2015)	ISO 9001:2015 sets out the criteria for a quality management system and can help to identify and address risks associated with an organization's supply chain management	C
19	International Organization for Standardization (ISO) ISO/IEC 15408 Common Criteria ISO	The Common Criteria for Information Technology Security Evaluation is an international	B

NUMBER	BODY, STANDARD	FUNCTION	THREAT GROUP
	15408-1:2009 (version 1: 12/2009; version 2: 6/2011; version 3: 6/2011)	standard for computer security certification, and is a useful guide for the development, evaluation and/or procurement of IT products with security functionality	
20	BSA - The Software Alliance BSA Framework for Secure Software Version 1, April 2019 [See Item 31, NIST)	Guidance on enhancing the integrity and security of software against malicious attack and on securely managing the selection, integration, and validation of third-party software components and component supply chains.	D
21	SAFECODE The Framework for Software Supply Chain Integrity (2009)	Provides a framework and common taxonomy for analyzing and describing the efforts of software suppliers to mitigate potential compromise of software during sourcing, distribution, or development	D
22	SAFECODE Managing Security Risks Inherent in the Use of Third party Components (2017)	Guidance for identifying, assessing and managing the security risks associated with the use of third-party components, and describes methods to sustain, test, improve, and quantify the security of third-party components when vulnerabilities are discovered	D
23	SAFECODE Fundamental Practices for Secure Software Development (2018)	Provides best practices for development of cloud-based and online services, shrink-wrapped software and database applications, as well as operating systems, mobile devices, embedded systems and devices connected to the Internet	D
24	SAE International Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition (AS5553C) (2019)	Standardizes practices to: maximize availability of authentic parts, procure parts from reliable sources, assure authenticity and conformance of procured parts, control parts identified as counterfeit, and report counterfeit parts to other potential users and government investigative authorities	A

NUMBER	BODY, STANDARD	FUNCTION	THREAT GROUP
25	DHS CBP: Customs – Trade Partnership Against Terrorism (C-TPAT) DHS/CBP/PIA-013 | C-TPAT Privacy Impact Assessment (PIA)	Supported by the 'Security and Accountability for Every Port Act of 2006', and is a voluntary public-private partnership where individual businesses enter into agreements with Customs to protect the supply chain, identify security gaps, and implement specific security measures and best practices	G
26	American Institute of Certified Public Accountants (AICPA) SOC Suite of Services – SOC for Service Organizations: Trust Services Criteria (2015)	A report on controls at a service organization. Help to evaluate an organization's information systems relevant to security, availability, processing integrity, confidentiality, and privacy	C
27	Department of Defense DFARS 252.246-7007 Contractor Counterfeit Electronic Part Detection and Avoidance System (2016)	DoD DFARS establishing contractor responsibilities for detecting and avoiding the use or inclusion of counterfeit electronic parts or suspect counterfeit electronic parts, the use of trusted suppliers, and requirements for contractors to report counterfeit electronic parts and suspect counterfeit electronic parts	A
28	Department of Defense DFARS 252.246-7008: Sources of Electronic Parts (2018)	Establishing rigorous requirements regarding the sourcing and provenance of electronic components for IT products purchased by DOD, intended to mitigate the potential for counterfeit components	A
29	National Institute of Standards and Technology (NIST) NIST SP 800-161 Supply Chain Risk Management (2015) (Rev. pending)	Comprehensive analysis and guidance to federal agencies on techniques to implement program of total life cycle ICT supply chain risk management	I
30	National Institute of Standards and Technology (NIST) NIST IR 7622 Notional Supply Chain Risk Management Practices for Federal Information Systems (2012)	Providing a set of practices to help federal departments and agencies integrate ICT supply chain risk management considerations into procurement of ICT systems, products, and services	D

NUMBER	BODY, STANDARD	FUNCTION	THREAT GROUP
31	National Institute of Standards and Technology (NIST) NIST SP 800-193 (Platform Firmware Resiliency Guidelines) (2018)	Provides principles and guidelines that can support platform firmware resiliency based on principles of Protection, Detection, and Recovery, primarily against remote attacks	D
32	National Institute of Standards and Technology (NIST) NIST SP 800-147 (BIOS Protection Guidelines) (2011)	Provides Security guidelines and management best practices for BIOS systems	D
33	National Institute of Standards and Technology (NIST) NIST SP 800-147b (BIOS Protection Guidelines for Servers) (2014) [See item 19 [ISO 19678]	Specifies security guidelines for four system BIOS security features: - Authenticated BIOS update mechanisms - An optional secure local update mechanism - Firmware integrity protections, to prevent unintended or malicious modification of the BIOS - Non-bypassability	D
34	National Institute of Standards (US) & CSE (CCCS) (Canada) FIPS 140-2 (effective 15-Nov-2001) Security Requirements for Cryptographic Modules (Rev. 2014)	Providing a standard and schema for testing conformance of cryptographic modules, ensuring that cryptographic components of systems used throughout the US federal space are implemented correctly	A
35	National Institute of Standards (US) & CSE (CCCS) (Canada) FIPS Pub 199: Standards for Security Categorization of Federal Information and Information Systems (2004)	Provides standards to be used by all federal agencies to categorize information and information systems collected or maintained by each agency	C
36	National Institute of Standards (US) & CSE (CCCS) (Canada) FIPS PUB 200: Minimum security Requirements for Federal Information and Information Systems (2006)	Specifies minimum security requirements (as directed by FISMA) for federal information systems other than classified or national security systems, as defined	B
37	NIST and OMB Statutory Authorities and Responsibilities under Federal Information Security Modernization Act of 2002 (FISMA)	Establishes roles and responsibilities of federal agencies, specifically including NIST and OMB, with respect to information systems standards, audits, and reporting. Requires that agencies and all IT service providers adhere to security	C

NUMBER	BODY, STANDARD	FUNCTION	THREAT GROUP
		control frameworks, conduct annual reviews, and report status to OMB	
38	NIST and OMB Statutory Authorities and Responsibilities under Federal Information Security Modernization Act of 2014 (P.Law 113-283)	Amends FISMA to establish roles and responsibilities of NIST, OMB and DHS with respect to information systems standards, audits and reporting. Reestablished the oversight authority of the Director of OMB with respect to agency information security policies and practices and sets for authority for DHS to administer implementation of those policies and practices	C
39	Federal Risk and Authorization Management Program (FEDRAMP) established under OMB memo 12/8/2011.	Provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by the U.S. Government, and implemented standard security baselines and processes to provide initial authorization of cloud service and a mechanism for security package to be reused across the Federal Government	C
40	Committee on National Security Systems: CNSS 505 Supply Chain Risk Management	Provides guidance and responsibilities for establishing an integrated, organization-wide cybersecurity risk management program for organizations that own, operate, or maintain NSS	D

3.2.1 FEDERAL INVENTORY OF SUPPLY CHAIN RISK MANAGEMENT EFFORTS

Task Force representatives have been working closely with OMB and the FASC to compile a federal version of the inventory, which will be released in the near future.

SECTION IV — WORKING GROUP 1: INFORMATION SHARING

Working Group 1 (WG1) focused on bi-directional information sharing. It was established to explore a common framework for how the Federal Government and industry can more effectively share actionable supply chain risk information.

Cyber threat indicators of compromise are generally more standardized in format, and, in many cases, are machine readable. Uniquely, supply chain risk information has less uniformity around “packaging” and delivery mechanisms. These characteristics heighten the need to effectively share risk information.

Actionable risk information may include identified product-based risks such as counterfeit products, device impersonation, and malicious code insertion. It may also include organizational risks, such as insider threat activities and physical attacks against participants or products in the supply chain.

WG1 leveraged the threat compendium compiled by WG2 to help inform development of meaningful and actionable reports for key stakeholders. Members reviewed more than 70 potential threats, considered which information would be most valuable in mitigating those threats, and assessed if that information was accessible to ICT stakeholders.

Actionable information often requires a level of specificity which may create sensitives about how it is shared. Critically, WG1 concluded that effective information sharing may necessitate the exchange of sensitive vendor or supplier data, including the names of specific entities. This need creates a range of legal considerations that ICT stakeholders must navigate and which the WG proposes for further study in the following phases of work.

4.1 Working Group Focus

WG1 efforts to date have focused on the following fundamental questions:

- What supply chain information would be most valuable in mitigating risk?
- Does that information exist in a manner/forum that can be accessed and leveraged for risk management purposes?
- If valuable information does not exist in an accessible manner/forum, what barriers might impede the collection and/or dissemination of such information?

The goal of the effort was to understand what supply chain threat information could provide insights to change, adapt, or modify supply chain risk postures. WG1 sought to share supply chain threat information in a way that enables corrective actions as a result of successful information exchanges. It was **not** created simply with the goal of information sharing for the sake of awareness only.

4.2 Working Group Outcomes & Activities

WG1’s first phase of activities largely addressed foundational and precursor issues surrounding supply chain information sharing paths and processes. In particular, issues of law and policy pertaining to information sharing between, and among, industry participants and government representatives dominated discussions.

WG1 determined that many types of risk information are available, but the sources were little known, not affordable, or not easily accessible. Since the threats to the supply chain are varied and diverse, no single repository of supply chain risk information can accommodate all facets of supply chain risk. As such, accessing and utilizing risk information is resource-intensive and, consequently, must be prioritized based on risk.

Upon additional review and analysis of the supply chain threat vectors, WG1 observed that the information of highest value in mitigating risk pertains to suspected, known, and/or proven bad actors. Correspondingly valuable information relates to specific threats to information technology/operational technology products, software, or services. WG1 sought to determine where this valuable information resided, noting that the most likely sources of information that could identify "suspect" supplier behavior would be drawn from primarily industry sources.

While there are some mechanisms in place for industry to disclose suspect supplier behavior, legal issues have been identified in sharing and/or receiving potentially derogatory, supplier-specific information. Even in trusted-group or not-publicly-accessible environments, industry is hesitant to share potentially derogatory information. Industry representatives have expressed concern that such sharing could expose sharers and recipients to legal risks from both government (federal or state) laws and from private litigation. WG1 noted that the Cybersecurity Information Sharing Act and the Critical Infrastructure Information Act provide potentially pertinent statutory information protections. However, WG1 also noted that these protections may not fully accommodate risks created by the type of information sharing that is the subject of WG1's deliberations. This remains an open issue about which the Working Group has not formed any conclusions.

4.2.1 INFORMATION SHARING WORKING GROUP REPORT

WG1's activities culminated in a report detailing background, methodology, observations, analysis, challenges, and recommendations related to information sharing in supply chain risk management. WG1 identified and categorized prerequisite issues and barriers into legal, process, and financial categories.

The Report highlighted the importance of sharing the most valuable information, including the lists of suspect suppliers and relevant information for mitigating these risks. The Report shared relevant information relating to the value of this information and the barriers that exist to acquiring and acting upon these information sources.

WG1 concluded that legal analysis and guidance are a prerequisite to developing a framework for any systematic, omni-directional information sharing system relating to suspect suppliers. The result of these legal considerations could set forth the guidelines for addressing the process, operational, and financial barriers that restrict effective implementation.

> *The Working Group sought to drive effectiveness by focusing on making information actionable. That translates into evaluation of how to address challenges around identifying "bad actors" and how to mitigate risk of suspect suppliers.*

4.3 Future of the Working Group

WG1 has identified the following recommended potential next steps for information sharing, largely focused on addressing and resolving legal constraints and considerations going forward:

- Identify a small, relevant set of key government agency and private sector representatives with specific subject matter expertise on the legal issues relating to supply chain information sharing barriers identified in the Working Group 1 Report;
- Incorporate review by relevant parties, as well as independent counsel, to ensure the successful assessment of legal barriers and potential avenues for mitigating these risks; and
- Leverage those considerations to create a specific recommendation from the private sector members of the Task Force that can be delivered to government representatives and other interested

stakeholders within the duration of the Task Force. This recommendation could address potential legislative and/or regulatory efforts to resolve potential legal issues identified in the Working Group Report. These recommendations could then be shared with the FASC for its evaluation.

SECTION V – WORKING GROUP 2: THREAT EVALUATION

Working Group 2 (WG2), the Threat Evaluation Working Group, was established to identify processes and criteria for threat-based evaluation, focusing on the types of threats that can create mission impacts. It focused on the ICT supplies, products, and services. Importantly, WG2 concentrated on threat evaluation, rather than risk assessment, ensuring it looked more broadly at the SCRM ecosystem rather than risks associated with individual assets

The processes and resulting insights developed by WG2 serve as a baseline evaluation of SCRM threats, providing invaluable insights for mitigating risk. Moreover, they may be utilized as guidance on the application of the NIST risk management framework.

5.1 Working Group Focus

WG2 first identified and inventoried broad groups of ICT supply chain threats, then gathered additional information for those threats, establishing threat scenarios to provide context for evaluation. The Working Group Co-chairs leveraged the National Institute for Standards and Technology (NIST) Risk Management Practices described in NIST SP 800-161 to help guide the analysis of the threats and threat sources identified in this initiative.

The activities of WG2 ultimately inform the efforts of the other Task Force WGs. For example, the threats identified by WG2 have been used to inform the Information Sharing WG1 by providing focus areas for information gathering and sharing. Similarly, the identified threats support assessment of the inventory of standards and best practices that may be applicable to the evolving Counter-SCRM threat environment (see Section 3.2).

5.2 Working Group Outcomes & Activities

WG2 has developed several products over its first phase of work that support continued discussion and facilitate decision-making in the next phase of work. These products are discussed below.

5.2.1 INVENTORY OF THREATS

WG2 solicited inputs from its members to generate an inventory of threats for evaluation. WG2 then used the categories defined in “Supply Chain Risk Management Practices for Federal Information Systems and Organizations” (NIST SP 800-161) to capture additional information to characterize these threats, such as the threat’s source and event description, among others.

Use of the NIST document resulted in a work product that is consistent with NIST guidance and flexible enough to be used by industry and public sector for a variety of purposes.

5.2.2 THREAT MODELING: THREAT CATEGORIES AND SCENARIOS

The threat listing was developed through inputs from WG members and validation through broader Task Force engagement. It incorporates a model of threat sources and scenarios, which members provided. The identified SCRM Threats were then compiled and evaluated by WG members.

The Threat List was carefully broken down into nine categories that provide the framework for the threats and guided the inputs of the members:

- Counterfeit Parts
- Cybersecurity

- Internal Security Operations and Controls
- Compromise of System Development Life Cycle (SDLC) Processes and Tools
- Insider Threat
- Inherited Risk (Extended Supply Chain)
- Economic
- Legal
- External End-to-End Supply Chain

This categorization was refined into a defined group of supply chain threat groupings that will ultimately be able to support risk-informed decision making through improved awareness and threat mapping activities. This process has established a solid threat source evaluation that can be extended for specific products or services to drive evaluation of risks within the supply chain.

The Working Group developed an inventory of threats, setting the stage for creation of threat scenarios. These resources provide a key baseline on threat evaluation and provide the foundation for improving risk-informed decision-making.

Using the prior inputs, the WG then developed several threat scenarios that illustrated and provided valuable context for the Threat List and Threat Groups described above. Example threats were provided to address the fields identified in NIST SP 800-161. Scenarios provided background information on the threat itself, the importance of the threat, and potential impact on the supply chain. Each scenario provides relevant information that illustrates risk and provides supporting guidance, helping support decision-making at an entity or strategic guidance level. Where appropriate, each scenario included the following information:

- Background information and contextual support
- Threat source
- Vulnerability information
- Threat event descriptions
- Outcomes
- Organizational units & processes affected
- Potential mitigation strategies and SCRM controls

5.3 Future of the Working Group

WG2 focused on threat evaluation to build a model that assessed relevant information about the broad groups of threats facing ICT SCRM. This initial effort focused only on threats to suppliers. Next steps for the Working Group could include conducting a similar assessment with respect to products and services and result in a work product using specific threat scenarios for products and services.

WG2 focused on threat evaluation using specific risk areas. Using the NIST Risk Management Framework described in NIST SP 800-161, one potential subsequent step is to use scenario planning and continued WG efforts to document options for application of the threat scenarios to specific Risk Assessments.

SECTION VI – WORKING GROUP 3: QUALIFIED BIDDER LISTS & QUALIFIED MANUFACTURER LISTS (QBL/QML)

Working Group 3 (WG3) was established for the "identification of market segment(s) and evaluation criteria for Qualified Bidder and Manufacturer List(s)." While lists of Qualified Bidders and Manufacturers (QBL/QML) are a common practice in industry and government purchasing activities, the criteria for factoring in the appropriate supply chain risk issues is one of emerging importance and use. WG3 was tasked with providing realistic, actionable, economically feasible, and risk-oriented recommendations surrounding the use of QBLs/QMLs.

6.1 Working Group Focus

The WG's goal was to propose a method by which QBL/QML can be leveraged to help mitigate ICT supply chain risk through the inclusion or exclusion from entity procurements of individual products or product vendors. This inclusion or exclusion of parties are based on such considerations as vendor debarment data, past performance data, company or country of origin, or other identified qualifying or disqualifying law enforcement or intelligence information.

The initial proposed scope for WG3 was to address three questions:

- What is the recommended process for determining the type of ICT that should be on an approved list?
- What is the recommended type of ICT that a list should be established for?
- What are the recommended evaluation criteria for the list?

That scope has been refined over time to include the following:

- Understanding the current landscape for using QBL/QML in government procurement of ICT products and services today and whether/how they consider supply chain threats;
- Developing a set of factors to help inform an organization's decision to build or rely on a QBL/QML for ICT products and services;
- Taking the supplier threat evaluation criteria and categories identified by WG2 and applying it to the list of factors to identify opportunities for improvement; and
- Identifying or developing use cases where QBLs/QMLs are appropriately leveraging SCRM evaluation criteria.

The WG's objectives evolved from the initial collection of factors to consider when building a list to collectively assessing criteria for when QBLs/QMLs may be advantageous to securing the supply chain. Finally, WG3 is considering the development of a maturity model to help create a predictable and repeatable way to attain a level of trust in a product or source of supply that is commensurate with an assessed level of criticality and risk.

6.2 Working Group Outcomes & Activities

WG3 addressed current policies, practices, and gaps in the procurement of ICT products and services, as it relates to vendor qualification, using tools such as QBLs and QMLs. WG3 has facilitated briefings with subject matter experts on the current requirements for qualified lists and examined multiple use cases of QBLs and QMLs. The WG hosted/co-hosted four briefings that aligned with ongoing WG3 and WG4 efforts:

- Briefing on the Continuous Diagnostic & Mitigation (CDM) Approved Products List (APL)
- Briefing on GSA Schedule 70 Category Management

- Briefing on the NASA Solutions for Enterprise-Wide Procurement (SEWP)
- Briefing on NIST Standards 800-161, 800-53A, and 800-37

Industry participants' regular information sharing and discussion with government acquisition experts facilitated the development of recommendations to collectively address risks that impact the entire ecosystem. Through internal discussions and incorporation of a wide range of materials, the WG refined its approach to more effectively assess criteria for when, and how, to best deploy QBLs/QMLs.

6.2.1 DRAFT DELIVERABLE REPORT

WG3 developed a draft deliverable report that includes discussion of approaches to supply chain assurance, examples of current supply assurance programs, and recommended next steps. Completing the inventory and publishing the initial guidance from WG2 are the prerequisites for WG3 to ensure that identified key gaps are addressed through policy recommendations.

> *The Working Group has refined its approach to more effectively assess and identify criteria for when and how to best deploy QBLs/QMLs.*

The WG3 Report further lays out key next steps for improving and refining the guidance around development and use of QBLs/QMLs. It sets the stage for future use of the ICT SCRM Inventory (see Table 3) to conduct overviews of use cases, for conducting gap analysis on existing use case structures, and the opportunity for future study of trust-building product and supplier approaches. It articulates the options available to the ICT community and improves understanding of the challenges surrounding this process.

6.2.2 FACTOR LIST

WG3 identified an initial series of factors that could be used by entities to evaluate when considering the application of a QBL/QML. While not exhaustive, the list provided an initial framing structure to help stakeholders better understand the applicability of QBL/QMLs in "buying down" supply chain risk management. The list included the following factors and supporting questions:

- **Amount the entity spends** on the covered article
  - What is the total cost of ownership?
- **Market conditions** of the covered article
  - Is the covered article a commodity with many available sources or a customer covered article or a covered article with limited sources?
  - What is the transaction cost for changing suppliers?
  - What is the cost of sustainment (such as the frequency and complexity of updates to the covered article and other monitoring and support costs)?
  - How is end-of-life considered?
- **Importance of the covered article** to entity's goal/mission accomplishment
  - If this covered article fails, what is the impact to the entity's ability to achieve its goal(s)?
  - Is the covered article on existing critical asset lists or supporting critical functions, such as the High Value Asset (HVA) list, Agency Mission Essential Functions, etc.?
- **Frequency of known attacks** to or through the covered article or its supply chain

    - What is the likelihood of attack through the item to the supply chain?
- **Probability of threat** or the likelihood of an attack to the supply chain.
- **Level of Control** over the Manufacturing and Distribution of the covered article.
    - Are the potential sellers limited to original equipment manufacturers (OEMs), or OEMs and their approved distributors with appropriate security (e.g. anti-counterfeit) policies?
    - Is the equipment potentially sourced from a wide range of uncontrolled sources or distributors with widely varying security policies (e.g. online resellers)?
- **Volume of known vulnerabilities** in the covered article or in common configuration(s) of the covered article
- **Ease of compromise/vulnerability** of the covered article
- **Existence of standards** applicable to the covered article (NIST, ISO, etc.)
- **Existence of policy mechanisms** applicable to the covered article
- **Liability** if the covered article is compromised

6.3 Future of the Working Group

WG3 has identified the following potential next steps for the next phase of the Task Force's efforts. These could include the following steps to continue development of WG3's mission and advance further integration of the Working Group policy recommendation:

- Gaining an understanding of the current landscape for using QBL/QML in government procurement of ICT products and services today. It could also work to understand whether or how these entities consider supply chain threats;
- Finalizing and publishing a set of factors with the aim of helping to inform an organization's decision to build or rely on a QBL/QML for ICT products and services;
- Identifying or developing use cases where QBLs/QMLs are appropriately leveraging SCRM evaluation criteria; and
- Applying supplier threat evaluation criteria and categories identified by WG2 to the identified Factor List to identify opportunities for improvement and assessing of potential expansion.

SECTION VII – WORKING GROUP 4: POLICY RECOMMENDATIONS TO INCENTIVIZE PURCHASE OF ICT FROM ORIGINAL EQUIPMENT MANUFACTURERS (OEM) OR AUTHORIZED RESELLERS

Working Group 4 (WG4) was established to produce policy recommendations that incentivize the purchase of ICT products and services from original equipment manufacturers (OEM) or authorized resellers. Its objectives of assuring product authenticity and integrity have a close relationship with those of WG3, which address QBL/QMLs. WG4 members provided broad representation from across the range of public and private stakeholders.

7.1 Working Group Focus

WG4's objective was to recommend measures to help ensure that ICT purchased and used by the government and critical infrastructure owners and operators is authentic and has not been tampered with or altered. Inauthentic end items and components often do not have the latest security-related updates, may not be built to the original equipment (or component) manufacturer's security or quality standards, and may be more susceptible to inclusion of malicious code, known and unknown weaknesses and vulnerabilities, or other unwanted functionality.

Counterfeit ICT (hardware and software) and Internet of Things devices and systems present a challenge for manufactures from an intellectual property and brand management perspective. There are further problems for end users from an operational integrity and cyber risk perspective. OEMs have a heightened interest in ensuring the authenticity of their products, and this interest carries through into their policies for designating certain downstream suppliers or resellers as "authorized."

Industry often addresses the issue of product authenticity by limiting purchases of critical items to OEMs or authorized resellers. The Department of Defense has also adopted this policy and has implemented a rule in the DFARS (252.246-7007 *Contractor Counterfeit Electronic Part Detection and Avoidance System*) to require that purchases for critical systems be made only from OEMs or authorized resellers. Having a similar policy for the rest of the government would align with industry best practice and the DOD's purchasing approach.

7.2 Working Group Outcomes & Objectives

WG4 engaged in a series of meetings, workshops, and lines of effort to achieve its principal objective of delivering a policy recommendation on ICT purchasing from original manufacturers or their authorized resellers. The WG's discussions were supported by subject matter expert briefings to ensure that the WG's recommendation incorporated definitional work informed by leading industry practices and commercial standards. The policy recommendation is discussed below.

7.2.1 POLICY RECOMMENDATION

This WG delivered a policy recommendation that ICT be purchased from original manufacturers or their authorized resellers. The policy recommendation, fully titled *Procurement of Information and Communications Technology from Original Equipment Manufacturers, their Authorized Channels, or other Trusted Supplier(s),* incorporates a number of definitions circumscribing the term "authorized reseller" which include specific cyber and supply chain security requirements, informed by leading industry practices, the DFARS rule, commercial standards such as SAE AS6496 (*Authorized Distributor Anti-Counterfeiting Standard*), and ISO/IEC 20243 (*Information Technology -- Open Trusted Technology Provider Standard (O-TTPS)*). After the recommendation was unanimously agreed to by the Task Force Executive Committee, it was subsequently transmitted to the FASC.

The Working Group leveraged the broad representations of its members to successfully deliver a policy recommendation on OEM purchasing, accomplishing key foundational steps to inform future work.

7.3 Future of the Working Group

The primary tasking of the WG has been achieved with the delivery of the policy recommendation. In a next phase of work, WG4 may shift its focus to developing scoping documents for possible future Phase II work items, including providing scoping insights into potential topics for future consideration. Some of the proposed topics for future Task Force efforts that would build upon or leverage the efforts of WG4 could include the following:

- Identifying educational opportunities and key learning objectives per role involved in a holistic SCRM Program; and
- Developing potential standardized templates for vendors to describe or attest to their SCRM practices.

SECTION VIII – FUTURE OF THE ICT SCRM TASK FORCE

The Task Force's first year of efforts have created a foundation for tangible and operational improvements to policy approaches to improve ICT supply chain risk management. These first efforts have established the strategic foundation necessary to inform additional actionable solutions in next phases of work. The Task Force's recommendations set the stage for continued efforts to develop and implement initiatives to address both tactical and strategic measures to improve global ICT risk management.

8.1 Task Force Direction

As the Task Force moves into the next phase of its efforts, it will continue to evolve and grow, reflecting the ongoing changes in the broader supply chain risk management ecosystem. It will look to build upon its earlier work, while adapting both its focus areas and structure to address new challenges and issue areas.

The Task Force will conduct a comprehensive evaluation of its Working Group structure and conduct strategic planning efforts that drive creation of new or reconfigured Working Groups. It will follow a process similar to its previous work in identifying and selecting ideas for Working Groups, utilizing surveys and discussion sessions to gather inputs from the Task Force membership and trusted subject matter experts. New Working Group focus areas will largely fall into the following four categories:

- Inputs and recommendations from Working Groups in Phase 1 that can build on their work or address gaps or issue areas that were identified during Phase 1;
- Recommended topic areas considered but not selected during Phase 1 that might be more suitable for Phase 2, reflecting the changes in supply chain risk management ecosystem, progressing maturity of Task Force efforts, or timeliness of potential components;
- New topic areas gathered from Task Force members at large; and
- FASC-identified areas of support or study.

The Task Force will evaluate how it can best ensure that its recommendations are actionable and timely. It will continue to utilize collaborative processes to ensure the broad utility of its impact and that it reflects the needs, expertise, and capabilities of both government and industry. As it continues to determine how best to build upon its Phase 1 work and to fully set the stage for its next Phase, it will continue to identify potential subject matter experts who can contribute to its strategic planning and direction setting. This will include soliciting inputs from other critical infrastructure sectors, where appropriate, about potential experts or opportunities for improved connectivity.

The Task Force will further look to continue its coordination with the FASC. As the FASC grows and matures, the Task Force will be ideally situated to provide key insights and actionable support that help advance the FASC.

SECTION IX – CONCLUSION

Addressing SCRM requires ongoing, dedicated focus. The work developed by the Task Force in its first Phase will inform ongoing efforts, including, the FASC, other whole of government and partnership engagements, and the continued work of the Task Force itself.

The Working Groups have made progress in addressing longstanding concerns and situating the Task Force for continued success in the next phase of its work.

These successes demonstrate that the Task Force and its WGs stand as testimony to the importance of the concept of public-private partnerships underlying the CIPAC structure and its collaborative model. Particularly, the joint efforts of members from the Information Technology and Communications Sector Councils, combined with government counterparts, resulted in the creation of a unique body of diverse expertise from which to base the deliberations and conclusions produced by year one's initial efforts. All participants share a confidence that this approach, supplemented by continuing efforts to expand the outreach of the Task Force's engagements, will pay dividends in both the continuing quality of its future work and the capacity of this broad and diverse body to provide meaningful approaches that resolve long-vexing ICT supply chain risk challenges.

APPENDIX A: DEFINITIONS

5G: Fifth generation mobile network, whose specification the ITU has not fully defined. 5G is expected to support 10 gigabits per second data rates and higher. Standards for 5G network and mobile hardware proposed by the 3GPP standards coalition have been widely supported internationally under the rubric of "5G NR" (New Radio). (Newton's Telecom Dictionary)

Covered Articles: For the purposes of its work, the Task Force relied on the definition of "covered articles" provided in the Federal Acquisition Supply Chain Security Act of 2018.[8]

Critical Infrastructure: economic sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Assets may be owned by government or by private sector. (PPD 21)

Critical Infrastructure Protection Advisory Council (CIPAC): CIPAC is a DHS chartered advisory council that provides a forum that enables members of the recognized government coordinating councils (GCCs) and sector coordinating councils (SCCs) to discuss joint critical infrastructure matters for the purpose of achieving consensus on policy, advice, and recommendations to be presented to the Federal Government. (CIPAC Frequently Asked Questions)

Federal Acquisition Security Council: An interagency council, chaired by OMB, with authorities and functions described in subchapter III of chapter 13 of Title 41, United States Code. The Council's functions including identifying or developing criteria for sharing information with federal agencies, other federal entities, and non-federal entities with respect to supply chain risk and making recommendations to specified senior officials, for application to executive agencies or any subset thereof, regarding the exclusion of sources or covered articles from any executive agency procurement action or the removal of covered articles from executive agency information systems. (SECURE Technology Act, P.L. 115-390, Title II (Federal Acquisition Supply Chain Security Act of 2018), 41 U.S.C. §§ 1321-28.

ICT: Information and Communications Technology: the category of electronic systems consisting of voice and data networks and appliances and associated software and supporting services which create, process, store and transfer data of any form, including analog and digital voice, imaging, and text. (ITU)

ICT Supply Chain: Linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of ICT products and services and extends through development, sourcing, manufacturing, handling, and delivery of ICT products and services to the acquirer. (NIST)

ICT Supply Chain risks: Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (NIST SP 800-161)

ICT Supply Chain threat: An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss. Regardless of the specific term used, the basis of asset loss

[8] "Covered article" is defined as: i. information technology, as defined in section 11101 of Title 40, U.S. Code, including cloud computing services of all types; ii. Telecommunications equipment or telecommunications service, as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153); iii. The processing of information on a federal or non-federal information system, subject to the requirements of the Controlled Unclassified Information program; and iv. Hardware, systems, devices, software, or services that include embedded or incidental information technology. 41 U.S.C. § 4713(k)(2).

constitutes all forms of intentional, unintentional, accidental, incidental, misuse, abuse, error, weakness, defect, fault, and/or failure events and associated conditions. (NIST SP 800-160)

ICT Supply Chain vulnerability: Weakness in an element of the supply chain supporting the development or production of an information system, component, device, software and associated system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (NIST SP 800-37, NIST SP 800-161)

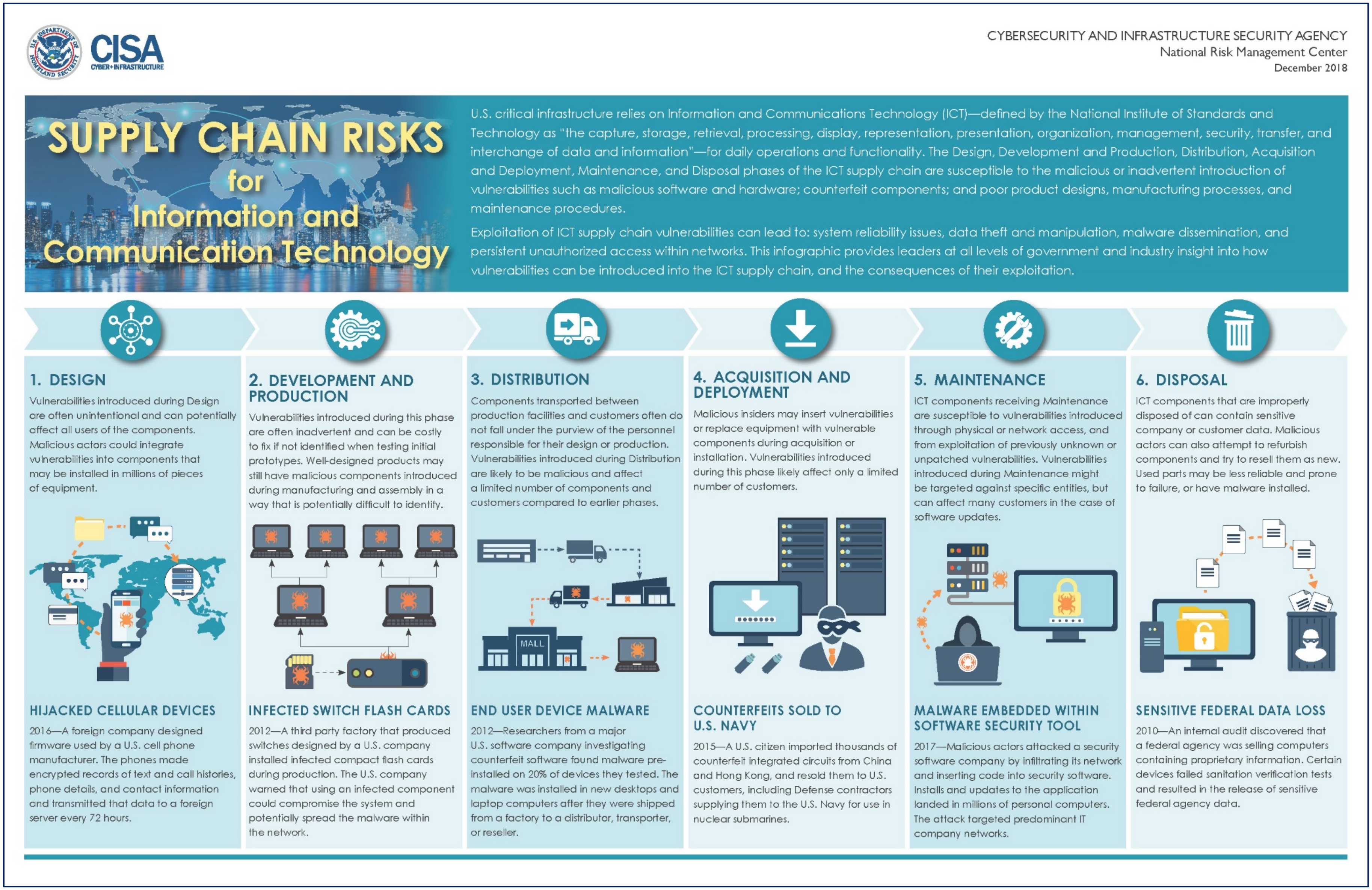
Supply Chain Risk Management: (SCRM) The process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of product and service supply chains. (NIST)

As applied to information systems, SCRM refers to the process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (1) the conduct of a risk assessment; (2) the implementation of a risk mitigation strategy; and (3) employment of techniques and procedures for the continuous monitoring of the security state the information system. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

ICT Supply Chain Risk Management (ICT SCRM): The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains. (NIST SP 800-161)

Cyber Supply Chain Risk Management: (C-SCRM) The process of applying SCRM techniques, tools and processes to that portion of ICT risk specifically attributable to the software or software dependent device elements of information technology systems. (Software/Supply Chain Assurance Forum)

APPENDIX B: ILLUSTRATING RISK TO THE ICT SUPPLY CHAIN



CISA
CYBER+INFRASTRUCTURE

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
National Risk Management Center
December 2018

SUPPLY CHAIN RISKS for Information and Communication Technology

U.S. critical infrastructure relies on Information and Communications Technology (ICT)—defined by the National Institute of Standards and Technology as "the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information"—for daily operations and functionality. The Design, Development and Production, Distribution, Acquisition and Deployment, Maintenance, and Disposal phases of the ICT supply chain are susceptible to the malicious or inadvertent introduction of vulnerabilities such as malicious software and hardware; counterfeit components; and poor product designs, manufacturing processes, and maintenance procedures.

Exploitation of ICT supply chain vulnerabilities can lead to: system reliability issues, data theft and manipulation, malware dissemination, and persistent unauthorized access within networks. This infographic provides leaders at all levels of government and industry insight into how vulnerabilities can be introduced into the ICT supply chain, and the consequences of their exploitation.

1. DESIGN

Vulnerabilities introduced during Design are often unintentional and can potentially affect all users of the components. Malicious actors could integrate vulnerabilities into components that may be installed in millions of pieces of equipment.

HIJACKED CELLULAR DEVICES

2016—A foreign company designed firmware used by a U.S. cell phone manufacturer. The phones made encrypted records of text and call histories, phone details, and contact information and transmitted that data to a foreign server every 72 hours.

2. DEVELOPMENT AND PRODUCTION

Vulnerabilities introduced during this phase are often inadvertent and can be costly to fix if not identified when testing initial prototypes. Well-designed products may still have malicious components introduced during manufacturing and assembly in a way that is potentially difficult to identify.

INFECTED SWITCH FLASH CARDS

2012—A third party factory that produced switches designed by a U.S. company installed infected compact flash cards during production. The U.S. company warned that using an infected component could compromise the system and potentially spread the malware within the network.

3. DISTRIBUTION

Components transported between production facilities and customers often do not fall under the purview of the personnel responsible for their design or production. Vulnerabilities introduced during Distribution are likely to be malicious and affect a limited number of components and customers compared to earlier phases.

END USER DEVICE MALWARE

2012—Researchers from a major U.S. software company investigating counterfeit software found malware pre-installed on 20% of devices they tested. The malware was installed in new desktops and laptop computers after they were shipped from a factory to a distributor, transporter, or reseller.

4. ACQUISITION AND DEPLOYMENT

Malicious insiders may insert vulnerabilities or replace equipment with vulnerable components during acquisition or installation. Vulnerabilities introduced during this phase likely affect only a limited number of customers.

COUNTERFEITS SOLD TO U.S. NAVY

2015—A U.S. citizen imported thousands of counterfeit integrated circuits from China and Hong Kong, and resold them to U.S. customers, including Defense contractors supplying them to the U.S. Navy for use in nuclear submarines.

5. MAINTENANCE

ICT components receiving Maintenance are susceptible to vulnerabilities introduced through physical or network access, and from exploitation of previously unknown or unpatched vulnerabilities. Vulnerabilities introduced during Maintenance might be targeted against specific entities, but can affect many customers in the case of software updates.

MALWARE EMBEDDED WITHIN SOFTWARE SECURITY TOOL

2017—Malicious actors attacked a security software company by infiltrating its network and inserting code into security software. Installs and updates to the application landed in millions of personal computers. The attack targeted predominant IT company networks.

6. DISPOSAL

ICT components that are improperly disposed of can contain sensitive company or customer data. Malicious actors can also attempt to refurbish components and try to resell them as new. Used parts may be less reliable and prone to failure, or have malware installed.

SENSITIVE FEDERAL DATA LOSS

2010—An internal audit discovered that a federal agency was selling computers containing proprietary information. Certain devices failed sanitation verification tests and resulted in the release of sensitive federal agency data.