INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT

CYBERSEC 2022

Katie Willers
September 2022

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

CISA partners with industry and government to understand and manage risk to our Nation's critical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

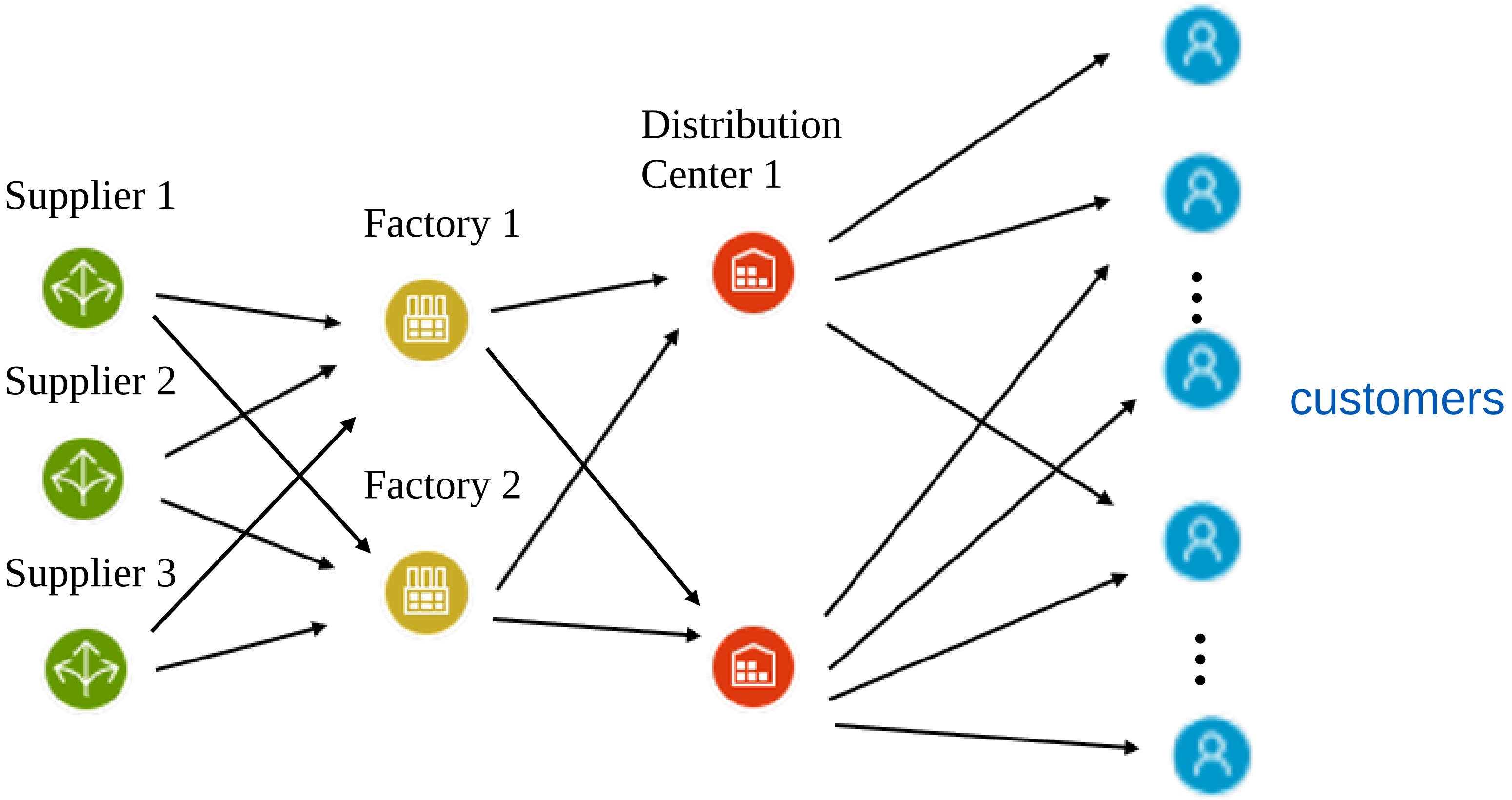
GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

months | years | decades

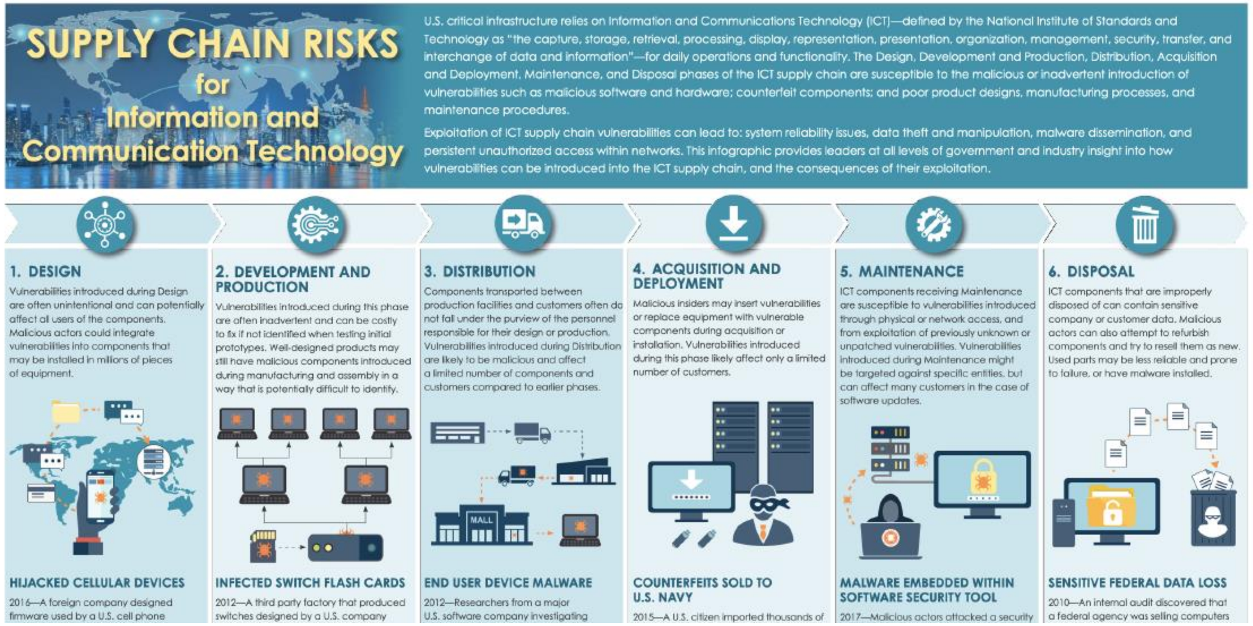
What is a Supply Chain?



Challenges for the ICT Supply Chain

- All aspects of our lives are intertwined with ***information and communications technology (ICT)***:
  - Smartphones and tablets
  - Laptops
  - Servers running our
    power grid and our financial transactions

- Threats include:
  - Counterfeit components
  - Cyberattacks
  - Introduction of malicious software
  - Ransomware



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.

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.

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.

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.

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.

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.

HIJACKED CELLULAR DEVICES

2016—A foreign company designed firmware used by a U.S. cell phone

INFECTED SWITCH FLASH CARDS

2012—A third party factory that produced switches designed by a U.S. company

END USER DEVICE MALWARE

2012—Researchers from a major U.S. software company investigating

COUNTERFEITS SOLD TO U.S. NAVY

2015—A U.S. citizen imported thousands of

MALWARE EMBEDDED WITHIN SOFTWARE SECURITY TOOL

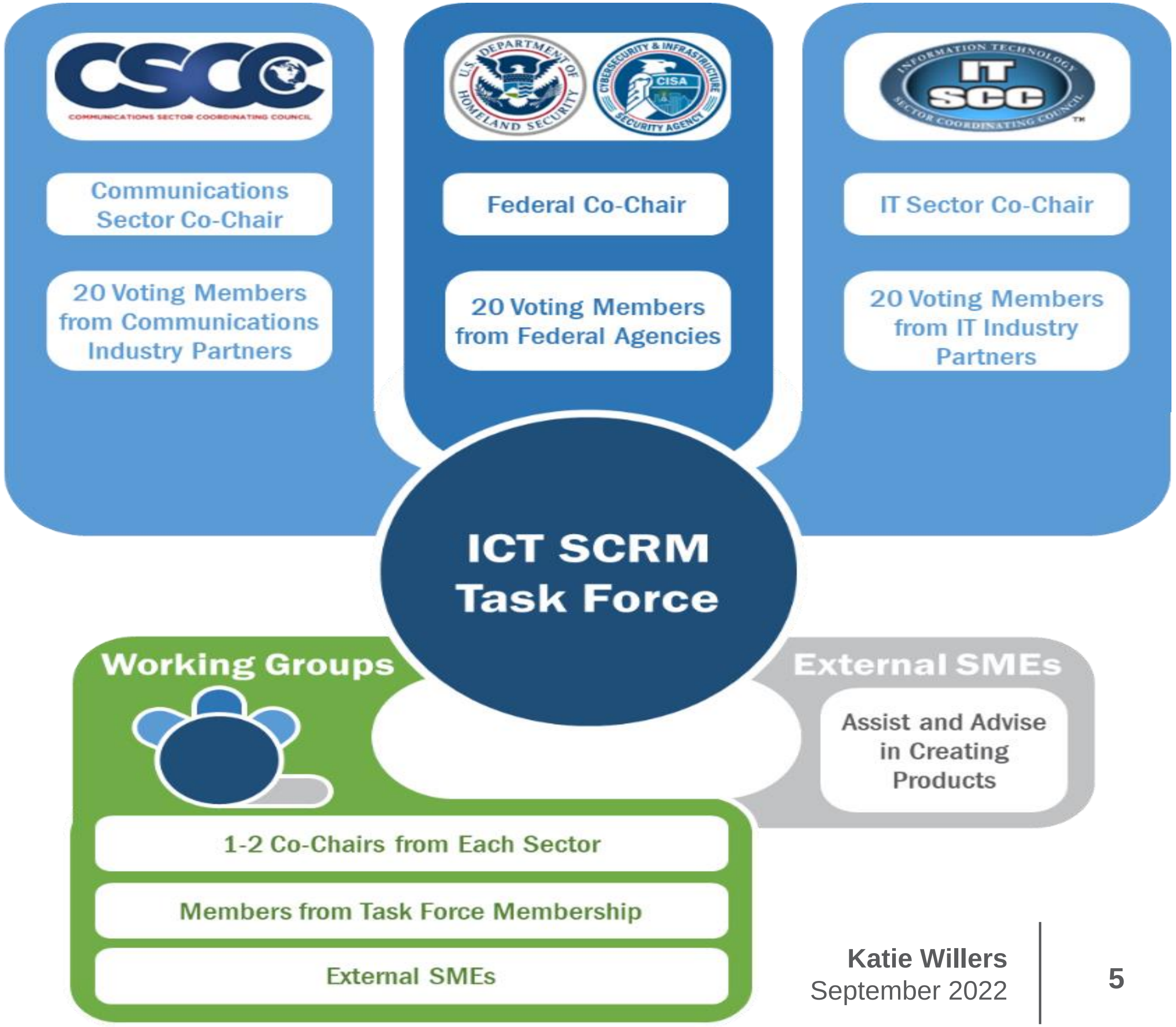
2017—Malicious actors attacked a security

SENSITIVE FEDERAL DATA LOSS

2010—An internal audit discovered that a federal agency was selling computers

Building Collective Supply Chain Resilience

Public-private partnerships are central to CISA’s collective defense approach to address the most significant risks to the Nation’s critical infrastructure. As such, CISA established the Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force, which is composed of professionals from the government and the Information Technology and Communications Sectors.



Communications Sector Co-Chair

20 Voting Members from Communications Industry Partners

Federal Co-Chair

20 Voting Members from Federal Agencies

IT Sector Co-Chair

20 Voting Members from IT Industry Partners

ICT SCRM Task Force

Working Groups

- 1-2 Co-Chairs from Each Sector
- Members from Task Force Membership
- External SMEs

External SMEs

Assist and Advise in Creating Products

ICT SCRM Task Force Focus Areas

Since its establishment, the Task Force has focused its work on:

- Legal, process, and financial barriers to sharing supply chain risk information
- Taxonomies to talk about the supply chain threat landscape in a more standardized manner
- Vendor templates that provide insight into the trust and assurance levels of ICT vendors
- Supply chain impacts from the COVID-19 pandemic
- Concerns of the small and medium-sized business community
- Examination of hardware and software bill of materials
- Software assurance
- Providing subject matter expertise to CISA for the development of key products or the execution of responsibilities related to executive orders and other national priorities

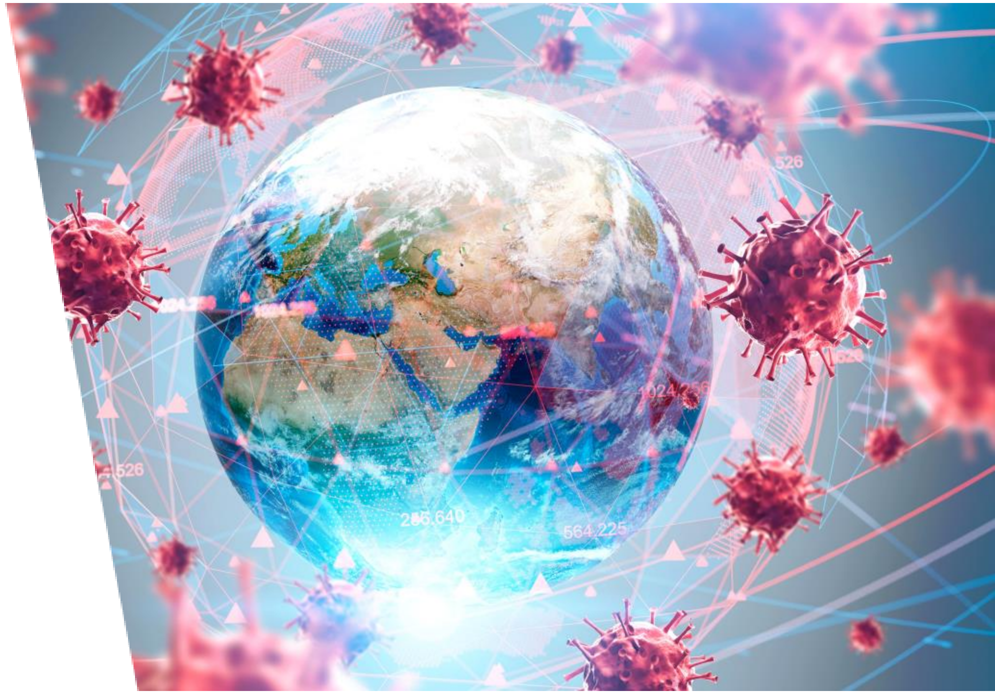
Lessons Learned: COVID-19

In its analysis report, *Building A More Resilient ICT Supply Chain: Lessons Learned During The COVID-19 Pandemic*, the ICT SCRM Task Force identified three key issues that impacted the ICT supply chain due to the pandemic:

- Reliance on single-source suppliers
- Reliance on lean inventory models
- Issues around supply chain transparency and understanding where junior tier suppliers are located

In addition to these broad lessons learned, the pandemic also brought about more specific supply chain issues:

- Tangible shortages of critical products
- Risks around logistics and transport
- Concerns about manufacturing and warehousing



ICT SCRM Risk Categories

ICT is integral for the daily operations and functionality of U.S. critical infrastructure. Due to the global distribution and interconnected nature of ICT, vulnerabilities to the ICT Supply Chain could have cascading impacts across multiple critical infrastructure sectors.

Risk Categories

- Counterfeit Parts
- External Attacks on Operations and Capabilities
- System Development Life Cycle (SDLC) Processes and Tools
- Inherited Risk (Extended Supplier Chain)
- Legal Risks
- Internal Security Operations and Controls
- Economic Risks
- External End-to-End Supply Chain Risks (e.g., Natural Disasters, Geo-Political Issues)
- Insider Threats

ICT SCRM Risk Categories

ICT is integral for the daily operations and functionality of U.S. critical infrastructure. Due to the global distribution and interconnected nature of ICT, vulnerabilities to the ICT Supply Chain could have cascading impacts across multiple critical infrastructure sectors.

Risk Categories

- Counterfeit Parts
- External Attacks on Operations and Capabilities
- System Development Life Cycle (SDLC) Processes and Tools
- Inherited Risk (Extended Supplier Chain)
- Legal Risks
- Internal Security Operations and Controls
- Economic Risks
- External End-to-End Supply Chain Risks (e.g., Natural Disasters, Geo-Political Issues)
- Insider Threats

ICT SCRM Risk Categories

ICT is integral for the daily operations and functionality of U.S. critical infrastructure. Due to the global distribution and interconnected nature of ICT, vulnerabilities to the ICT Supply Chain could have cascading impacts across multiple critical infrastructure sectors.

Risk Categories

- Counterfeit Parts
- External Attacks on Operations and Capabilities
- System Development Life Cycle (SDLC) Processes and Tools
- Inherited Risk (Extended Supplier Chain)
- Legal Risks
- Internal Security Operations and Controls
- Economic Risks
- External End-to-End Supply Chain Risks (e.g., Natural Disasters, Geo-Political Issues)
- Insider Threats

ICT SCRM Risk Categories

ICT is integral for the daily operations and functionality of U.S. critical infrastructure. Due to the global distribution and interconnected nature of ICT, vulnerabilities to the ICT Supply Chain could have cascading impacts across multiple critical infrastructure sectors.

Risk Categories

Counterfeit Parts

External Attacks on Operations and Capabilities

System Development Life Cycle (SDLC) Processes and Tools

Inherited Risk (Extended Supplier Chain)

Legal Risks

Internal Security Operations and Controls

Economic Risks

External End-to-End Supply Chain Risks (e.g., Natural Disasters, Geo-Political Issues)

Insider Threats

Understanding Supply Chain Threats

As technology evolves, so does the threat environment. The consequences of an ICT supply chain threat can extend beyond the initially targeted organization to its larger ecosystem of vendors, supplies, and customers and ultimately impact national security and economic resilience.

Threat Scenarios Report

- Provides practical, example-based guidance on supplier SCRM threat analysis and evaluation that can be applied by acquisition/procurement personnel and others who manage supplier, product, and service lists.
- This product was developed using feedback from end users and stakeholders to develop a lexicon compartmentalized into nine categories.
- Features sample scenarios with mitigation controls intended to help organization strengthen their security posture from the risks these threats pose to government and industry.

TLP: WHITE

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

INFORMATIO
TECHNOLOG
MANAGEME

Threat Evaluation V

February 2020

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT TASK FORCE

Threat Evaluation Working Group: Threat Scenarios

Version 2.0

January 2021

Assessing ICT Trustworthiness

Protecting critical information requires understanding not only the immediate supply chain, but also the extended supply chains of vendors and suppliers. To help organizations and businesses verify the trustworthiness of their supply chains, CISA's ICT SCRM Task Force developed the following resources:

VENDOR SUPPLY CHAIN RISK MANAGEMENT (SCRM) TEMPLATE

Vendor SCRM Template

This template provides a set of questions regarding an ICT supplier/provider's implementation and application of industry standards and best practices that can help guide supply chain risk planning in a standardized way. The template provides organizations clarity for reporting and vetting processes when purchasing ICT hardware, software, and services.

MITIGATING ICT SUPPLY CHAIN RISKS WITH QUALIFIED BIDDER AND MANUFACTURER LISTS

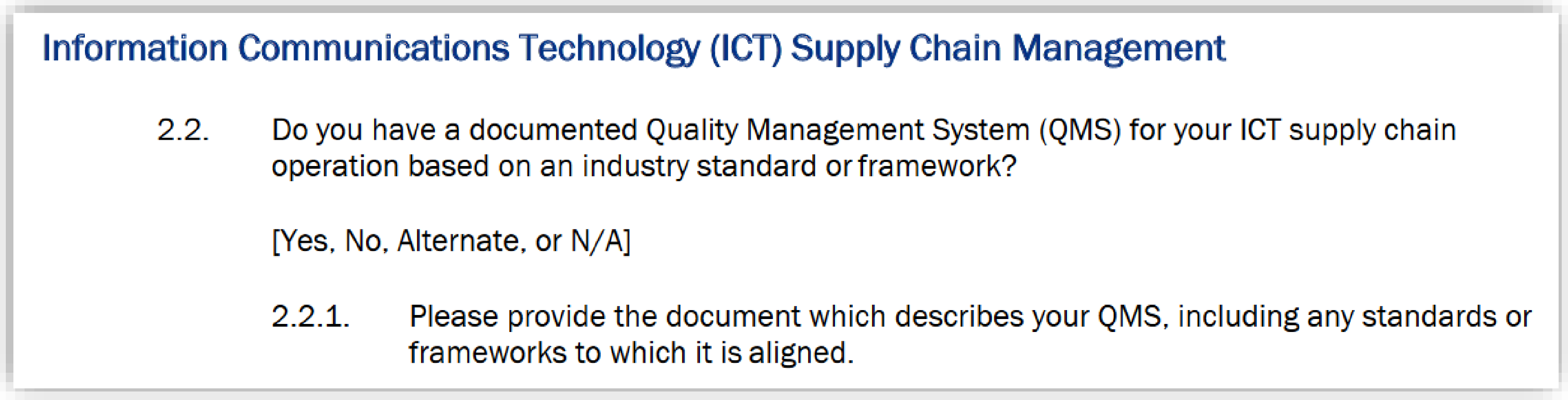
Recommendations on the Use of Qualified Lists and Considerations for the Evaluation of Supply Chain Risks

Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists

This report provides organizations a list of criteria and factors that can be used to inform an organization's decision to build or rely on a qualified list for the acquisition of ICT products and services.

ICT SCRM Vendor Template

- The ***Vendor SCRM Template*** was developed by the ICT SCRM Task Force to allow stakeholders to better assess the trustworthiness of ICT vendors and provide organizations with clarity for reporting and vetting processes when purchasing ICT hardware, software, and services.
- The template provides a set of questions regarding an ICT supplier/provider’s implementation and application of industry standards and best practices that can help identify policy gaps and guide supply chain risk planning in a standardized way.
- A sample question from the template:



Information Communications Technology (ICT) Supply Chain Management

2.2. Do you have a documented Quality Management System (QMS) for your ICT supply chain operation based on an industry standard or framework?

[Yes, No, Alternate, or N/A]

2.2.1. Please provide the document which describes your QMS, including any standards or frameworks to which it is aligned.

Providing Guidance for SMBs

Engaging with the small and medium-sized business (SMB) community fuels a need to understand their unique needs and tailor SCRM products to make them more applicable to SMBs. This guide is the first step towards the Task Force helping to improve the supply chain risk posture of SMBs:

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

OPERATIONALIZING THE VENDOR SUPPLY CHAIN RISK MANAGEMENT TEMPLATE FOR SMALL AND MEDIUM-SIZED BUSINESSES

September 2021

CSCC
COMMUNICATIONS SECTOR COORDINATING COUNCIL
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
INFORMATION TECHNOLOGY
IT SCC
SECTOR COORDINATING COUNCIL

Operationalizing Vendor SCRM Template for Small and Medium-sized Businesses

Tailors the previously described enterprise Vendor SCRM Template for use by SMBs. The product provides guidance on applying industry standards and best practices for reporting and vetting processes when purchasing ICT hardware, software, and services.

Accompanying Spreadsheet

An easy-to-use spreadsheet version; this is as an alternate tool to utilize this product and is intended to accommodate yes, no, or partial responses to each of the questions.

ICT SCRM Resources

Below are a few of the informational products CISA has developed to raise awareness of supply chain vulnerabilities. For a complete list of resources, please visit: cisa.gov/supply-chain. And please email any questions to ict_scrm_taskforce@cisa.dhs.gov.

SCRM Essentials

A guide for leaders and staff with actionable steps on how to start implementing organizational SCRM practices to improve their overall security resilience.

Threat Scenarios Report v3

Identifies the processes and criteria for threat-based evaluation of ICT suppliers, products, and services.

ICT Supply Chain Risk Management Toolkit

Identifies the processes and criteria for threat-based evaluation of ICT suppliers, products, and services.

Vendor SCRM Template

Provides organizations with a set of questions to help enhance clarity for reporting and vetting processes when purchasing ICT hardware, software, and services.

Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacture Lists

Provides organizations a list of criteria and factors that can be used to inform an organization's decision to build or rely on a qualified list for the acquisition of information and communications technology (ICT) products and services.

For more information:

cisa.gov/supply-chain

Questions?

ict_scrm_taskforce@cisa.dhs.gov