CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

INFORMATION AND COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT TASK FORCE YEAR 2 REPORT

Status Update on Activities and Objectives of the Task Force

December 2020

This page is intentionally left blank.

FOREWORD

Over the past year, the Nation has lived through a challenging pandemic. Much of society is living, working, and interacting in ways that are different than anticipated, and relying on Information and Communications Technology (ICT) in new ways. This new environment has created fundamental shifts in ICT's interactions with the systems, operations, and functions upon which we rely. The ICT Supply Chain Risk Management Task Force (ICT SCRM Task Force) was created to improve the Nation's collective ability to assess and mitigate threats to the ICT supply chain and improve the security and resilience of those supply chain elements and systems. Over its first two years, the Task Force has been and continues to play an invaluable role in addressing key areas of supply chain concern.

We are particularly proud that the Task Force has proven itself so resilient over the past several months—transitioning to fully remote operations and continuing to collaborate and highlight its value by producing high-quality recommendations, analysis, and work products. The Task Force continues to serve as a key convening point for government and industry, and its ability to incorporate and assess the foundational shifts to the ICT supply chain landscape is a testament to the enduring value of these types of partnering efforts.

In this Report, we are pleased to highlight the work being done by the Task Force and its Working Groups over the last year. In particular, the Working Groups have built upon their past work and forged linkages between their work to create a more cohesive set of products and recommendations that provide a holistic approach to improving supply chain security and resilience. Work relating to information sharing feeds into work developing recommendations on threat analysis, which, in turn, provides an essential foundation for the efforts relating to creating vendor assurance and trust mechanisms, including qualified bidder and qualified manufacturer lists. This complementary approach across Working Groups is a key element of the unified, beneficial outcomes the Working Group provides.

This Report highlights the positive outcomes the Task Force has generated in its first two years. We look forward to our continued work together addressing new challenges, maximizing the impact of what we have accomplished already, and improving the efficacy of supply chain security and resilience efforts.

Thank you to all of our dedicated Task Force members, the participants who volunteer their time and expertise to help make the Task Force a success, and the supply chain stakeholders who have been essential partners in planning, developing, and executing the Task Force's efforts.

December 2020

Government Co-Chair: Bob Kolasky
CISA Assistant Director, National Risk Management Center

Industry Co-Chair: John Miller
Information Technology Sector Coordinating Council

Industry Co-Chair: Robert Mayer
Communications Sector Coordinating Council

EXECUTIVE SUMMARY

Information and communications technology (ICT) is integral to the daily operations and functionality of the United States' economy and national security. The risk environment facing these systems, assets, and stakeholders necessitates continued efforts to grow security and resilience through coordination, deployment of expertise, and the creation of critical resources and tools. Since its inception, the ICT Supply Chain Risk Management (SCRM) Task Force has been a forerunner and centerpoint of ICT risk management partnership activities. The Task Force provides for better awareness and understanding of the threat environment facing ICT supply chains and develops useful, actionable recommendations to bolster the networks that underpin infrastructure functionality.

Over the past year, the Task Force has expanded upon its first-year progress to advance meaningful partnership around supply chain risk management. Specifically, the Task Force:

- Developed reference material to support overcoming legal obstacles to information sharing
- Updated the Threat Evaluation Report, which evaluates threats to suppliers, with additional scenarios and mitigation measures for the corresponding threat scenarios
- Produced a report and case studies providing in-depth descriptions of control categories and information regarding when and how to use a Qualified List to manage supply chain risks
- Developed a template for SCRM compliance assessments and internal evaluations of alignment to industry standards
- Analyzed the current and potential impacts from the COVID-19 pandemic, and developed a system map to visualize ICT supply chain routes and identify chokepoints
- Surveyed supply chain related programs and initiatives that provide opportunities for potential Task Force engagement

Moreover, like the rest of the country, the Task Force faced unprecedented logistical challenges caused by the COVID-19 pandemic. Despite the disruptions to the Task Force and its operations, the dedication of the individual members and the companies that participate resulted in the continuation of work and completion of objectives. In recognition of and response to the disruptions caused by COVID-19, the Task Force stood up a new working group focused on analyzing the impacts of the COVID-19 pandemic on ICT supply chains.

This Year 2 Report presents highlights of the Task Force's accomplishments over the past year, highlighting where it has successfully built on its past work and providing information on the products, deliverables, and efforts produced by the Task Force Working Groups.

Contents

PARTICIPATING ORGANIZATIONS

Task Force membership represents a range of government and industry stakeholders, ensuring input from across both the public and private sectors. In addition to its voting membership, the Task Force receives extensive subject matter expert support from participants across the public, IT, and Communications sectors.

TABLE 1 — VOTING MEMBER ORGANIZATIONS

GOVERNMENT	IT SECTOR	COMMS SECTOR
Federal Bureau of Investigation	Accenture	AT&T
Federal Communications Commission	BSA	Charter Communications
Federal Energy Regulatory Commission	CyberRx	Comcast
General Services Administration	Cybersecurity Coalition	CompTIA
National Aeronautics and Space Administration	Cyxtera	Cox
Office of the Comptroller of the Currency	Dell	CTIA
Pennsylvania Chief Information Security Officer	FireEye	Ericsson
U.S. Department of Commerce	General Dynamics Information Technology	Iconectiv
U.S. Department of Defense	HP	Lumen
U.S. Department of Energy	IBM	National Association of Broadcasters
U.S. Department of Health and Human Services	Information Technology Information Sharing Analysis Center	NCTA
U.S. Department of Homeland Security	Information Technology Industry Council	NTT
U.S. Department of Justice	Intel	Pioneer
U.S. Department of the Treasury	Interos Solutions	TIA
U.S. Nuclear Regulatory Commission	Microsoft	T-Mobile
U.S. Office of the Director of National Intelligence	Palo Alto Networks	USTelecom
U.S. Social Security Administration	Samsung	Verizon Wireless
U.S. Department of State	Synopsys	

SECTION I — INTRODUCTION

Information and communications technologies (ICT) are integral for the daily operations of the American economy and national security. Vulnerabilities in the ICT supply chain, composed of hardware, software, and services from third-party vendors, suppliers, service providers, and contractors, could affect all users of that technology.

ICT components are also the foundational building blocks of a broad range of critical infrastructure systems. They underpin a broad range of National Critical Functions that our national and economic security, and public health and safety rely upon.

Confidence in these components and systems is critical, meaning security must be a centerpiece of their lifecycle, from their design, to development, to introduction and continued operation and monitoring. Vulnerabilities in supply chains—either developed intentionally for malicious intent or unintentionally through poor security procedures—enable several debilitating and dangerous threats, undermining system integrity and resilience. Disruption to the ICT Supply Chain could have far-reaching and potentially devastating impacts on infrastructure systems and operations far beyond the Information Technology (IT) and Communications Sectors, with the extensive private stake in ICT supply chain resilience potentially at risk.

The critical importance of the ICT supply chain highlights the invaluable role of the ICT Supply Chain Risk Management Task Force (Task Force). The Task Force builds upon natural linkages between government and private sector partners. This partnership uses collective action and collaboration to merge expertise, best practices, and resources between government, the IT Sector, and the Communications Sector.

Last year, the Task Force released a Year One report laying out the progress of the Working Groups and sharing key findings from initial efforts. As the Task Force nears the end of a second year of operations, this Year Two Report highlights the successes made over the past year by the Task Force and its constituent Working Groups, along with discussion of potential next steps and future items for consideration. The Task Force has continued to build on the work done in its first year and developed and shared a wider array of products, analysis, and information to help ICT stakeholders improve the security and resilience of their supply chains.

This Report summarizes the findings and efforts of the Working Groups, highlighted Task Force products, and identifies potential areas for continued Task Force work to continue to support SCRM efforts across government and industry.

- Section II provides a Task Force overview, structure, membership, and links to other SCRM efforts.
- Sections III through Section VII provide summaries of the efforts and objectives of the individual Working Groups, along with links to their work products
- Section VII details some of the potential options for future work of the Task Force that have been discussed as options for consideration.

The products created by the respective Working Groups that are available for public release can be found on www.cisa.gov/supply-chain.

SECTION II — TASK FORCE OVERVIEW

Chartered as a consensus-based body under the Critical Infrastructure Partnership Advisory Council (CIPAC), the Task Force's objectives include to:

- Act as a forum for collaboration with private sector owners and operators of critical infrastructure, through their respective sector coordinating councils (SCCs), on methods and practices to effectively identify, prioritize, and mitigate ICT supply chain risks
- Provide realistic, actionable, timely, economically feasible, scalable, and risk-based recommendations for addressing ICT supply chain risks
- Recommend methods to develop and implement initiatives, including mutually beneficial public-private partnerships, designed to improve risk management in global ICT supply chains

The Task Force embodies CISA's collective defense approach to cybersecurity risk management, as encapsulated in the work of CISA's National Risk Management Center (NRMC), which manages the Task Force.

TASK FORCE MEMBERSHIP

The ICT SCRM Task Force is a public-private collaboration that includes 60 members from federal agencies, the Communications SCC, and the Information Technologies (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:

- Bob Kolasky, CISA Assistant Director, represents government members
- Robert Mayer, CSCC Chairman, represents the Communications Sector
- John Miller, IT-SCC Vice-Chairman, represents the IT Sector

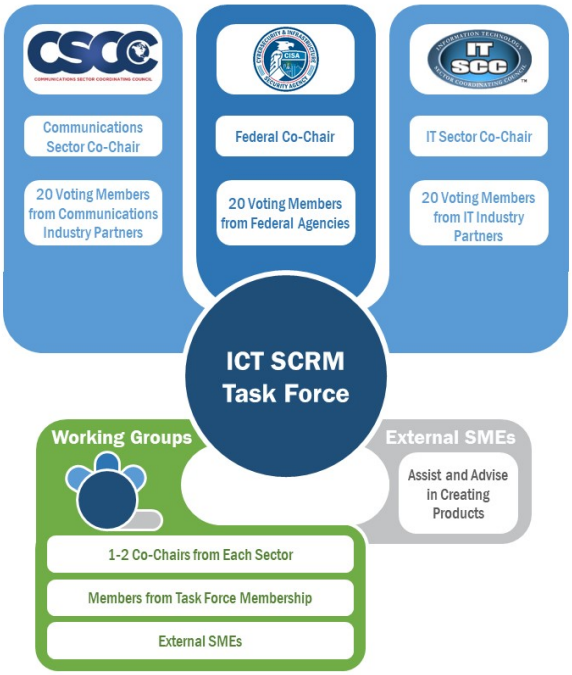

FIGURE 1 - THE ICT SCRM TASK FORCE STRUCTURE BLENDED INPUTS AND EXPERTS FROM ACROSS GOVERNMENT AND THE PRIVATE SECTOR

Members leverage the assistance and expertise of colleagues from their organizations to support Task Force efforts, as appropriate. As well, ICT subject matter experts from organizations not represented by the membership are included in working group activities upon approval by Task Force leadership. A range of stakeholders from across the public and private sectors provide invaluable contributions, expertise, and participation. 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. Members bring unique perspectives from both large and small organizations with roles in shaping supply chain risk management practices. Ultimately, the objective of this public-private partnership is to share recommendations and guidance proposed by the Task Force with industry and government stakeholders. Such a partnership guides all producers and consumers of ICT on methods to enhance their resilience and most effectively manage risks presented by the ICT supply chain. The list of participating organizations can be found in Table 1.

TASK FORCE PROGRAM AREAS

The ICT SCRM Task Force utilizes the National Infrastructure Protection Plan (NIPP) established partnerships, including the CIPAC structure, to facilitate information exchange between government, industry partners, and subject matter experts. This structure provides a flexible, trusted environment to engage parties to solve critical problems.

At the end of its first year of operations, the Task Force identified several topics of focus for its second year. The topics included both ideas that would augment or continue the work of Year 1 and new ideas solicited from members. To identify and prioritize Year 2 focus areas, the Task Force considered projects that:

- The Task Force is uniquely qualified to take on
- Address a clear gap in the current risk management environment
- Support the framing of policy and operational recommendations
- Will result in the greatest impacts
- Have a path to implementation

Using those criteria, the Task Force selected program areas of focus for Year 2, featuring efforts that represented logical continuations, expansions, and follow-ons to the work completed in Year 1. Each focus area was assigned to a Working Group for study. Additionally, in response to the global COVID-19 pandemic and its resulting impacts on the threat environment for ICT supply chains, the Task Force stood up a Working Group to analyze the impacts of COVID-19. As a result, the Year 2 constituent Working Groups were:

- **The Information Sharing Working Group (WG1)** tackled a discrete and important ecosystem wide challenge for supply chain risk management around barriers to bi-directional information sharing. The outcome will be relevant for all other Working Groups, but the legal examination efforts could occur with relative autonomy to the other groups
- **The Threat Evaluation Working Group (WG2)** catalogued the universe of threats to ICT supply chains and offer specific remediation and resilience activity (that map to existing frameworks and standards) to help reduce risk from those threats. This universe of supply chain threats started by looking through the lens of suppliers in Year 1, and then expanded to products and services in Year 2
- **The Qualified Bidder List/Qualified Manufacturer List (QBL/QML) Working Group (WG3)** created SCRM criteria for inclusion in qualified bidders and manufacturers list requirements and for application to various federal procurement use cases. The criteria that will help govern inclusion or exclusion on one of these lists can also be drawn from parts of the template created by WG4
- **The Vendor Supply Chain Risk Management (SCRM) Assurance Template Working Group (WG4)** created a flexible and agile template to answer key questions that collectively provide insight into the supply chain risk management posture of organizations. The questions distilled into this template build upon existing industry standards reflect collaboration with other Task Force working groups
- **The COVID-19 Impact Study Working Group (WG5)** studied supply chain operational topics such as inventory management, supply chain mapping/transparency, and supply chain diversity to understand impacts to organization's supply chains based on external events

These groups, in conjunction with the Coordination Tiger Team (see the "Connections Across the Public and Private Sector" section), provided an interconnected approach that blended the expertise and contributions of government and industry to build security and resilience. Figure 2 illustrates the connections between the Working Groups and highlight the unity of effort that was key to the success of the Task Force.

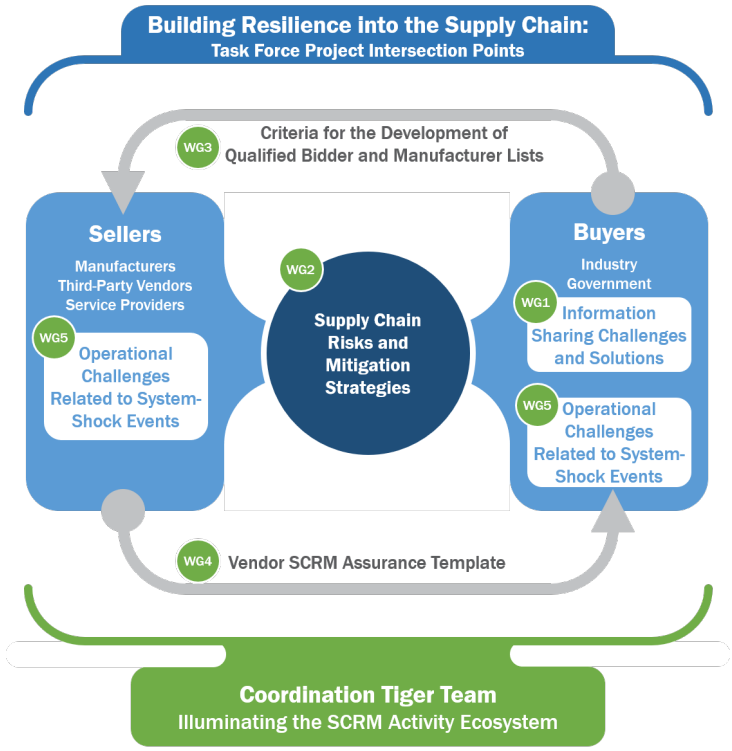

FIGURE 2 - THE TASK FORCE'S WORKING GROUPS WERE LINKED THROUGH COMMON EFFORTS

The Working Groups' collective effort addressed the lifecycle of supply chain risk management, from how stakeholders identify and understand risk, how they communicate about and work together to address risk, how they can grow their structural operations for addressing risks, and how they can improve their understanding and self-assessment of their risk posture. The Working Group topics reflected not only the areas of expertise and pressing concerns of Task Force members, but also an understanding of what issue areas could benefit from new tools, resources, or analysis for ICT supply chain stakeholders.

The Task Force recognizes the importance of creating flexible products that address the circumstances and needs of all stakeholders in the ICT supply chain. 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.

CONNECTIONS ACROSS THE PUBLIC AND PRIVATE SECTOR

The Task Force links stakeholders across the public and private sector, working to advance key issues in ICT supply chain security and resilience. The Task Force has made concerted efforts to explore and engage across the supply chain environment, identifying key opportunities to grow the impact and improve engagement.

FEDERAL ACQUISITION SECURITY COUNCIL (FASC)

The Task Force maintains close contact with the Federal Acquisition Security Council (FASC), with regular cross-entity briefings to provide awareness and identify potential coordination opportunities, as well as representation on the Task Force by FASC member agencies. The ICT SCRM Task Force develops strategic and operational recommendations to reduce supply chain risk that are shared with the FASC as well as other government bodies, such as the Federal Acquisition Regulatory (FAR) Council.

COORDINATION TIGER TEAM

Additionally, the Task Force created a Coordination Tiger Team to help members and Working Groups stay better informed about ongoing and nascent government and industry supply chain efforts, related to policy implementation and significant programmatic investments. Tiger Team members include representatives from each of the three participating Task Force entities (e.g., U.S. government, IT Sector Coordinating Council, Communications Sector Coordinating Council). The Tiger Team meets on a regular basis to share information on other supply chain risk management efforts that offer potential connection or engagement opportunities.

Tiger Team Objectives

The Tiger Team has grown the collective understanding of the broader SCRM environment and the lines of effort across the ICT landscape. The Tiger Team developed an inventory of major initiatives that included points of contact or other programs where the Task Force could benefit from engagement, as well as identified how

and when to share findings or proposed actions with the broader Task Force. This built connections to and improved understanding of other, potentially complementary, SCRM efforts.

Tiger Team Inventory

The Tiger Team conducted an environmental scan of relevant supply chain programs, initiatives, news, and guidance. The Tiger Team used a combination of multi-platform research efforts, news aggregation, and elicitation to broader supply chain stakeholders to build an inventory. This Inventory includes information, timelines, material on the relevance to the Task Force, and contact information for updates relating to the entries. Examples include:

- CISA Control Systems Interagency Working Group
- Federal Acquisition Security Council
- Bureau of Industry and Security (BIS) Entities List
- BIS De Minimis Regulation
- National Telecommunications and Information Administration Software Bill of Materials
- National Institute of Standards and Technology National Cybersecurity Center of Excellence Supply Chain Assurance Project
- Federal Communications Commission Final Designation Proceedings
- Relevant Executive Orders
- Department of Defense Cybersecurity Maturity Model Certification
- *National Defense Authorization Act*, Section 889, "Federal Acquisition Regulation Rule Implementation"
- Cyberspace Solarium Commission
- National Strategy to Secure 5G of the United States

SECTION III — WORKING GROUP 1: BI-DIRECTIONAL INFORMATION SHARING

The ICT SCRM Task Force established the Bi-Directional Information Sharing Working Group (hereafter, WG1) to explore a common approach for the federal government and industry to more effectively share supply chain risk information. WG1's efforts will support the working processes of the Federal Acquisition Security Council (FASC) and enhance omnidirectional information sharing among multiple stakeholders.

WG1's primary assumption is that the private sector will value and, most critically, act upon information shared about suspect suppliers. WG1 also assumed such sharing will be beneficial to the government, but its efforts focused on the private sector. WG1 developed an initial *Interim Information Sharing Report* outlining its methodology and recommendations for next steps.

In Year 2, WG1 built on those recommended next steps and expanded its work from Year 1, providing a more detailed analysis of specific issues raised in Year 1. WG1 developed a matrix describing litigation risk considerations and a series of potential approaches that could benefit sharing opportunities. This Executive Litigation Risk Awareness Matrix is a preliminary quick-look matrix of litigation risks to serve as a decision-support tool. This matrix is included in Appendix B.

GOAL AND OBJECTIVES

Informed by its initial year findings, WG1 concluded that it should undertake a discrete and time-limited effort to address legal issues with sharing derogatory, supplier-specific supply chain risk information to provide a framework for bidirectional sharing that protects companies as well as U.S. Government obligations and interests. Specifically, WG1 convened a small, relevant set of key government agency and private sector representatives with specific subject matter expertise regarding the legal supply chain barriers identified in the *Interim Information Sharing Report* to define and refine the specific barriers that must be overcome, and to identify methodologies to overcome these barriers.

YEAR 1 SUMMARY

WG1's initial interim report identified categories of supply chain risk information aligned to specific threats, together with the existence and ease of accessibility of such information. WG1 concluded that the information of most value to both private and public sectors was the exchange of supplier-specific risk creating information.

WG1 found that the potentially most valuable suspect-supplier information was likely discovered earlier by industry, not by government. More critically, WG1 concluded that the sharing of suspicions or concerns is hampered by legal concerns, namely the prospect of facing a private cause of action, most likely brought by the supplier about whom the concerns were raised. WG1 concluded that while certain statutory protections, such as those under Title I of the *Cybersecurity Information Sharing Act of 2015* and the *Critical Infrastructure Information Act of 2002*, may be pertinent to addressing these concerns, they did not fully accommodate the risks that information sharing creates.

OBJECTIVES

WG1 set out to provide an overview of the specific private litigation risks that may arise in the context of sharing derogatory, supplier-specific supply chain risk information.

OUTPUTS

WG1 developed its *Report and Recommendations on Reducing Private Litigation Risks Arising from the Sharing of Supply Chain Risk Information*, which was shared with the Task Force in August of 2020. The Task Force voted to approve that WG1 had accomplished its objectives, closing out the Working Group's efforts for the year. The Executive Litigation Risk Awareness Matrix from this report is included in Appendix B.

OUTCOMES

The WG1 report focused on three general categories of claims that can make information sharing about supplier risk difficult unless there is clear understanding of how to do so legally and mitigate the following:

- **Anti-Competitive Behavior:** Economic or business tort claims, such as tortious interference with business advantage
- **False Information:** Defamation or misrepresentation claims, such as business disparagement, defamation, and fraudulent misrepresentation
- **Breach of Obligations of Confidentiality:** Trade secret claims and breach of contract, including revealing practices, processes, designs, etc. that the manufacturer may assert are protected trade secrets, breach of nondisclosure requirements in a quote, contract, etc.

Ensuring that information sharing is done appropriately in a legal context was a goal of WG1 and its work centered around providing more clarity on how to legally share information about supply chain risks.

DELIVERABLES

WG1 and its members created three main deliverables that were shared with the Task Force. These deliverables consisted of:

- A table describing the key considerations for litigation risk that would arise in the context of seven specific claims in the previously listed categories
- A preliminary quick-reference matrix of private litigation risks relating to potential avenues for minimizing legal risks in sharing derogatory, supplier-specific supply chain risk information
- Several potential approaches to consider to enable beneficial sharing while mitigating the identified private litigation risk. These approaches span education and outreach regarding litigation risk mitigation, clarifying the desire for supply chain risk information sharing, and exploring additional longer-term changes in law

Analysis of Specific Private Litigation Risks

As noted, WG1 focused on three general categories of potential legal claims: anti-competitive behavior, false information, and breach of obligations of confidentiality. WG1 conducted analysis on the specific litigation risks that it identified through its process. Building on this analysis, WG1 developed the Executive Litigation Risk Awareness Matrix that provides an overview of the specific private litigation risks that may arise in the context of sharing derogatory supplier-specific supply chain risk information. The table provides a summary for each of seven different causes of action of the key considerations informing a risk analysis in the context of sharing derogatory supplier-specific supply chain risk information, from the viewpoint of a private sector entity that could face private suit.

The following are the seven causes of action highlighted by WG1:

1. Tortious Interference with Existing Contract
2. Tortious Interference with Prospective Contract, Business Relationship, or Business Advantage
3. Defamation
4. Business or Commercial Disparagement
5. Fraudulent Misrepresentation
6. Breach of Contract
7. Misappropriation of Trade Secrets

WG1 categorized the key considerations for a risk analysis relating to each cause of action, helping inform future efforts to develop measures that would mitigate the risks associated with information sharing under these causes of action.

Executive Litigation Risk Awareness Matrix

Private sector members of WG1, in conjunction with subject matter expertise from Federal stakeholders and Working Group participants, developed the Executive Litigation Risk Awareness Matrix—a preliminary quick-reference matrix of private litigation risk that illustrated how personnel who might encounter derogatory, supplier-specific supply chain risk information could work to minimize legal risks in sharing. This matrix does not in itself constitute legal guidance; instead, it highlighted an approach for providing preliminary awareness for the purpose of seeking legal advice and developing a sound approach to sharing. The matrix is offered as a discussion and decision-support tool to help inform ongoing conversations about information sharing approaches.

The Executive Litigation Risk Awareness Matrix can be found in Appendix B.

Analysis and Options Development

WG1 discussed several policy and legal options to encourage sharing of supply chain risk information. Improvements in public-private risk information sharing have grown more prevalent but those often focus on increasing cyber indicator threat sharing. This type of sharing was and is often accomplished through industry sector-specific information sharing and analysis centers (ISACs) and information sharing and analysis organizations (ISAOs). However, many companies were still concerned with the liability risk of sharing, similar to many of the risks discussed in previous sections. To alleviate these concerns, the government created policies to protect companies. The *Cybersecurity Information Sharing Act of 2015* provides liability protection for a narrow set of information to be shared with government and among companies. As well, authorities like Protected Critical Infrastructure Information and Critical Energy Infrastructure Information, provide confidentiality and liability protections for certain critical infrastructure information provided to the government.

In the same manner as cyber threat indicator sharing, policies to increase and improve supplier risk information sharing must balance business confidentiality, privacy, and competition with law enforcement and public safety considerations in the context of supply chain security. Creating the proper balance for supply chain issues deserves equal care to address similar societal concerns. For example, if the type of information to be shared is scoped too narrowly, organizations will limit sharing; but if it is scoped too broadly, it could lead to unfair competition actions in ways that do not aid law enforcement or national security goals.

WG1 conducted research and deliberations regarding approaches that could be used to create an environment that offers liability protections to companies who share supply chain risk information with the government and each other. These recommendations touch on a wide range of categories, looking to bolster a holistic approach to improving information sharing and strengthening broader supply chain security and resilience. Those recommendations included, but were not limited to the following topics:

- Providing education for key stakeholders on current supply chain threat information tools, resources, mechanisms, and opportunities. This would include working to build awareness of how to participate in, access, and provide documentation for information sharing opportunities, as well as mitigation measures to address the corresponding litigation risks
- Developing frameworks that can be used by private sector entities to engage with key government stakeholders and partners to request specific supply chain security risk information, including encouraging private sector partners to outline the potential benefits that could be derived from this information
- Identifying a centralized mechanism, entity, or process that could serve as a "clearinghouse" for sharable information on supply chain threats and risks. This entity could promulgate rules and best practices for sharing and protecting the information, both with the government as well as with other private sector entities, helping mitigate some legal risk
- Continued collaboration between government and industry to evaluate how potential statutory or regulatory changes could support mitigation of legal risks in supply chain threat information sharing

CONCLUSION

The ICT SCRM Task Force approved WG1's findings and recommendation in August 2020. The Executive Litigation Risk Awareness Matrix developed by the private sector members of Working Group 1, in conjunction with federal subject matter experts, can be found in Appendix B.

WG1 continues to work with the Task Force leadership to identify opportunities to implement recommendations and explore potential future efforts.

SECTION IV — WORKING GROUP 2: THREAT EVALUATION

The ICT SCRM Task Force established the Threat Evaluation Working Group (hereafter, WG2) to identify processes and criteria to evaluate supply chain threats to ICT suppliers, products, and services.

Supply chain risk managers can use these products to define supply chain threats to inform a mature risk management process. They are intended to provide practical, example-based guidance on supply chain risk management threat analysis and evaluation that can be applied by procurement or source selection officials in government and industry to assess supply chain risk and develop practices/procedures to manage the potential impact of these threats.

By extending WG2's Year 1 report to include products and services, the Threat Scenario development process continues to provide concrete examples that risk managers can use to inform procurement actions, such as the development of qualified supplier, product, or service lists by procurement officials in conjunction with the Qualified Bidder List and Qualified Manufacturer List (QBL/QML) Working Group's (WG3's) work product.

Over the course of Year 2, WG2 developed version 2.0 of the Threat Evaluation, incorporating new approaches and applying its prior work to products and services and incorporating potential threat mitigating strategies and possible SCRM controls to reduce threat impacts. These materials are available on the CISA website (www.cisa.gov/supply-chain), alongside the work from WG2 during Year 1.

GOAL AND OBJECTIVES

Building upon the objectives and goals from Year 1, WG2 conducted an assessment of threats to and from products and services, evaluating those threats with a scenario-based process. WG2 created a risk and mitigation resource by leveraging threat groupings and applying the National Institute of Standards and Technology (NIST) Risk Management Framework described in NIST SP 800-161. WG2 used scenario planning and continued efforts to develop potential mitigation measures for SCRM threats to incorporate into the final products.

YEAR 1 SUMMARY

WG2 was chartered with the goal to identify processes and criteria for threat-based evaluation of ICT supplies, products, and services. The objectives of this Threat Evaluation were defined as:

- Produce a set of processes and criteria for conducting supplier, product, and service threat assessments
- Focus processes and criteria on global ICT supplier selection, pedigree, and provenance
- Address product assurance (hardware, software, firmware, etc.), data security, and supply chain risks
- Establish a framework for a threat-based assessment of cyber supply chain risks that can be extended in future work products to address other critical infrastructure sectors

WG2 developed a Threat Scenarios Report that inventoried SCRM threats to suppliers against a categorization framework derived from NIST SP 800-161. It supplemented and validated that threat inventory with a series of threat scenarios that illustrated and provided context to the threat inventory and categorization efforts. These scenarios provided relevant information and supporting guidance relating to sources, vulnerabilities, threat events, outcomes, impacted units or processes, and potential mitigation efforts.

OBJECTIVES

The broad objectives guiding WG2's Year 2 work efforts focused on building on the successful processes and efforts of the work in Year 1. These objectives include building an inventory of threats by leveraging existing

resources and the expertise of its membership, sorting threats into categories, and developing scenarios to provide valuable context and guidance. This manifested in two specific goals:

- Conducting an assessment of SCRM threats to products and services by repeating and utilizing the Year 1 approach of the inventory and scenario-based process and building on the Year 1 findings
- Identifying and developing potential supply chain risk management mitigations for each of the threat scenarios developed in Year 1 and Year 2 through a scenario planning approach that uses the WG2 Year 1 efforts and the "Supply Chain Threat Scenarios and Analysis Framework" (Appendix D) in NIST SP 800-161 as guides

OUTPUTS

WG2 extended the Threat Evaluation to suppliers work-product from Year 1 to include products and services. The threat scenario development process provides concrete, practical examples for the threat scenarios that can be used to inform procurement actions, such as the development of qualified supplier, product, and service lists by procurement officials, in conjunction with WG3's work product.

Threat Evaluation Work

WG2 began work to build upon its prior threat evaluation work to apply its efforts more broadly. The WG built a threat list, which was validated and expanded through continued interaction with Task Force members, subject matter experts, and continued engagement. WG members considered C-SCRM threats identified from a variety of sources including Industry subject matter experts (SME), Department of Defense (DoD), Intelligence Community (IC), DHS, and others to inform the development of risk-based criteria. The first data call conducted was a request from WG membership to provide supply chain threats that they recognize from their own experience or from their organization's perspective. The threats identified by the WG members were consolidated and grouped to provide a set of threat groupings for further the development of specific scenarios.

WG2 provided the following deliverables over the duration of the ICT SCRM Task Force:

- **May 2020:** Risk Mitigation for Suppliers draft addendum to Phase 1 report
- **September 2020:** Risk Mitigation for Suppliers final addendum to Phase 1 report
- **October 2020:** Products and Services Threat Evaluation draft report
- **December 2020:** Products and Services Threat Evaluation final report

Each phased deliverable is a standalone report that builds upon the effort in the previous phases. WG2 chose to include these updates as a standalone report to benefit the audience by providing a complete report without the need to include numerous references to the original report. WG2 provided additional revisions to this report later in Year 2 to include supply chain risk management threat evaluations for products and services.

The categorized threats were consolidated into the following threat groups to aid the evaluation process:

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

WG2 achieved consensus on the definitions of *product* and *service* to ensure consistency within the Threat Evaluation Report.

For the WG2 Threat Evaluation Report, an *ICT product* is:

- a commercial end-item that stores, retrieves, manipulates, transmits, or receives information electronically in an analog or digital form.
    - **End-Item:** a system, equipment, or assembled commodity ready for its intended use
    - **Equipment:** a type of ICT that is comprised of a combination of parts, components, accessories, attachments, firmware, or software that operate together to perform one or more functions of, as, or for an end-item or system. Equipment may be a subset of an end-item based on the characteristics of the equipment. Equipment that meets the definition of an end-item is an end-item. Equipment that does not meet the definition of an end-item is a component
    - **Component:** any assembled element that forms a portion of an end-item

An ICT *service* is:

- An offering, or capability, or delivery of ICT functionality that does not require the user-or-customer to purchase, own, and operate the underlying ICT Product, or
- An offering, or capability, or delivery of manpower that directly supports an ICT Product to include the planning, design, implementation, operation, security, optimization, or life cycle support

Threat Scenario Mitigation Measures

In Year 2, WG2 added the assessment of impacts and mitigating controls to each of the Supplier Threat Scenarios released in Year 1. The edits expanded the existing scenarios by adding potential threat mitigating strategies and possible SCRM controls to reduce these threat impacts. These updates provide practical, example-based guidance on Supplier SCRM threat analysis and evaluation, helping better inform procurement decision-making and facilitating improvements in planning efforts to develop mitigation measures that bolster SCRM resilience. These modifications to the Supplier Threat Scenarios are reflected in the new Threat Scenarios.

These additional sections are included in Appendix C, Threat Scenarios, of version 2.0 of the Threat Scenarios Report.

CONCLUSION

WG2, focused on threat evaluation, completed version 2.0 of the Threat Scenarios Report to include the assessment of Impacts and Risk Mitigation for the Supplier Threat Evaluation from Year 1. Supply chain risk managers can use this work product to develop practical applications specific to supply chain risk management or as parts to inform a mature risk management process. The updated Threat Scenarios provide a non-exhaustive list of example supply chain threats, potential impacts, and associated mitigations. These scenarios are intended to be used as examples, and not as specific threats that every organization needs to mitigate as described in the example. The process of threat identification, impact analysis, and mitigating steps are core elements of the NIST Cybersecurity Framework and other applicable cyber risk management methodologies. This process is not specific to the ICT sector, it is applicable to all organizations that utilize risk management frameworks such as the NIST Cybersecurity Framework. It also established a solid threat source evaluation that can be extended for specific products or services to drive the evaluation of SCRM risk. The Task Force voted to approve the Threat Scenarios 2.0 at its September 30, 2020 Task Force meeting.

WG2's completed materials can be found through the CISA website (http://www.cisa.gov/supply-chain).

SECTION V — WORKING GROUP 3: QUALIFIED BIDDER LISTS/QUALIFIED MANUFACTURER LISTS (QBL/QML)

The ICT SCRM Task Force established the Qualified Bidder Lists (QBLs)/Qualified Manufacturer Lists (QMLs) Working Group (hereafter, WG3) to identify market segment(s) and cyber-SCRM (C-SCRM) evaluation criteria for QBLs and QMLs. Moreover, the group was established to study how QBLs and QMLs could be used and which market segments it is appropriate to use them in, particularly in terms of purchasing ICT products. A qualified list is a pre-approved list of the entities that provide an acceptable product or service for purchase, through the procurement process. The suppliers on that list would have already met a specified set of criteria, such as experience, standards, etc.

WG3 set out to do the following tasks:

- Serve as a reference source to raise awareness and educate both government and industry about the purpose and benefits of qualified lists for ICT products and services and the importance of building-in C-SCRM considerations
- Provide actionable recommendations to incorporate SCRM into new and existing ICT-related qualified list criteria and program processes
- Promote the use of security or assurance standards or criteria to evaluate ICT products or processes to develop or produce them
- Share best practices to educate the supply base and communicate expectations regarding suggested C-SCRM relevant vetting criteria to use in qualifying organizations/suppliers, especially if and when there is a need for a higher level of assurance that a source or product is trustworthy

During Years 1 and 2, WG3 analyzed five government programs that use QBLs, QMLs, and/or qualified (or approved) products lists (QPLs), as use case reviews. It discovered valuable insight into when and how to use a QBL/QML in government procurement and optimal categories of SCRM criteria and processes. WG3 scoped the focus of tasks to identify considerations for use of Qualified Lists to enhance C-SCRM.

The group has consolidated its findings and recommendations into a *Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists Report*, which can be found on the CISA website (http://www.cisa.gov/supply-chain).

GOAL AND OBJECTIVES

In Year 2, WG3 sought to build on the information gathered in Year 1 to develop a menu of evaluation criteria, grouped into categories of potential C-SCRM risk. The group also worked towards providing examples of specific criteria relevant to those categories, as well as considerations about whether and how to build a qualified list program to manage ICT supply chain risks.

YEAR 1 SUMMARY

In Year 1, WG3 refined its focus to:

- Understand the current landscape for using QBL/QML in government procurement of ICT products and services today and whether/how they consider supply chain threats
- Develop a set of factors to help inform an organization's decision to build or rely on a QBL/QML for ICT products and services
- Take the supplier threat evaluation criteria and categories identified by WG2 and apply them to the list of factors to identify opportunities for improvement
- Identify or develop use cases where QBLs/QMLs are appropriately leveraging SCRM evaluation criteria

By the end of Year 1, WG3 developed a draft deliverable report that included discussion of approaches to supply chain assurance, examples of current supply assurance programs, and recommended next steps.

OBJECTIVES

WG3's primary Year 2 objective was to iterate on Year 1 work to develop and provide realistic, actionable, economically feasible, and risk-based recommendations surrounding the use of "Qualified Lists" as one tool that can help organizations better manage ICT supply chain risk. In addition, the group focused on describing the purpose and benefits of including SCRM criteria in qualified lists to improve the use and management of qualified lists as an ICT SCRM management tool. By providing this information and a common set of control categories, the group sought to:

- Reduce C-SCRM risks associated with ICT
- Promote effective development and management of qualified lists
- Help officials make better decisions regarding when and how to use a qualified list

WG3 set out to produce a report that includes recommendations for consideration by policy and program officials and provides useful reference information and best practices for the broader ICT community. The WG3 report:

- Explains the purpose and benefits of qualified lists
- Provides a description of factors that inform a decision to build/rely on a QBL/QML for ICT products and services
- Proposes actionable recommendations for incorporating categorical SCRM considerations as qualification criteria related to one or more of the SCRM pillars listed in NIST SP 800-161 into new and existing ICT-related qualified list criteria and program processes

OUTPUTS

WG3 conducted use case reviews of five qualified list programs currently underway in various parts of the federal government. Analysis of these use case studies allowed the group to refine information regarding when and how to use a qualified list and begin developing its evaluation criteria and aligning these criteria to control categories. The group analyzed the following government programs:

1. DHS Continuous Diagnostics and Mitigation (CDM)
2. NASA Solutions for Enterprise-wide Procurement (SEWP)
3. Air Force and GSA 2nd Generation Information Technology (2GIT) blanket purchasing agreement
4. DOD Cybersecurity Maturity Model Certification (CMMC)
5. Federal Information Processing Standards (FIPS) 201 Evaluation Program and Approved Products List

WG3 examined any relevant SCRM criteria incorporated in those programs and cross-referenced them to the control categories in NIST SP 800-161. From there WG3 developed an overarching set of control categories, organized in parity with the NIST SP 800-161 controls and harmonized with the vendor template categories used by the SCRM Vendor Template Working Group (WG4).

Similar qualified list programs and processes exist for industry organizations, industry consortia, State Governments and others. While WG3 scoped its effort to examine Federal Government qualified list activities, the benefits, processes, and criteria described in the WG3 report are applicable to the broader ICT Community. WG3 includes an illustrative reference list of other (both Federal and non-Federal) Q-List programs in an Appendix to its new report.

WG3 presented these categories as part of its *Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists Report*, contextualized within the broader set of background, considerations, and guidance regarding the development of qualified lists assembled over the last two years. This report provides foundational information to help public and private sector decision-makers ensure C-SCRM criteria are included in qualifying activities and to more effectively use qualified lists as a tool to manage ICT supply chain risks.

WG3's methodology for analysis examined each program's specific SCRM requirements, drawing upon Requests for Quotations (RFQs) and other relevant documents. WG3 identified areas of overlap in

requirements across the various programs and performed a gap analysis of the use cases' overall approach to SCRM. Examining the threat categories created by WG2, WG3 mapped each category to the control categories found in the NIST SP 800-161 guidance. Using this information, WG3 reviewed how the SCRM requirements for each use case aligned with these control categories.

As part of a comprehensive supply chain risk management approach, organizations may require a higher level of confidence than a manufacturer or a bidder offering a service or a product are able to satisfy. A QBL/QML that incorporates C-SCRM qualification criteria can be an effective way to provide positive assurance that a business entity, and/or the products and services a business entity offers or produces, is sufficiently qualified to be considered an acceptable source of supply. Inclusion of C-SCRM considerations is especially important for QBL/QML associated with ICT products and services.

WG3 worked from a fundamental assumption that understanding the benefits of qualified lists and factors to consider before establishing a list would be of significant value to the private sector. WG3 also assumed considerations for incorporating SCRM into an ICT-related qualified list program would be beneficial to the government, but its primary assumption is that the private sector would value and, most critically, act upon QBLs and QMLs.

DELIVERABLES

In the *Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists Report*, WG3 included the following deliverables:

- Analysis of five case studies that led to the development of an overarching set of common ICT SCRM evaluation criteria control categories to be considered when building a qualified list program that, in whole or in part, seeks to manage supply chain risks
- A Year 2 report that includes in-depth descriptions of identified control categories and related foundational information regarding when and how to use a qualified list to manage supply chain risks

Recognizing that a one-size-fits-all approach to building a qualified list would not serve those relying on qualified lists, WG3 avoided developing a common set of evaluation criteria questions in favor of a menu of ICT SCRM control categories to be considered in relation to the list-builder's needs and objectives. Each of the categories mapped cleanly to the four pillars of supply chain risk outlined in NIST SP 800-161: security, integrity, resilience, and quality. Effectively addressing supply chain risks across the supply chain and life cycle of ICT requires that the protections in place for the bidder or manufacturer appropriately and adequately address the overlap of these pillars. The categories included the following, recognizing that these risk categories can be categorized under more than one pillar:

- Supply Chain Security
    - Physical Security
    - Cyber Security
    - Personnel Security (inclusive of Company leadership)
- Supply Chain Integrity
    - Hardware Integrity
    - Software Integrity
- Supply Chain Resilience
- Supply Chain Quality
    - Supply Chain Management & Supplier Governance

WG3 detailed these categories and sub-elements in its report, describing the relevant elements, QBL/QML development and utilization criteria, and relevant considerations and authorities for each element. This information is intended to help decision-making and execution around QBL/QML efforts by driving incorporation of one or more of these "pillars" as components of ICT qualified lists.

WG3's updated report also provided examples of the use cases that could be utilized in describing SCRM resilience criteria for incorporation into QBL/QML efforts. These use cases highlight the justifications, descriptions, evidentiary requirements, verification processes, and relevant standards and governance that are identified in utilizing particular criteria. The following are some example use cases that describe SCRM resilience criteria that could be incorporated into a Qualified Bidder List or Manufacturer List, highlighting the linkage between a justification and the underlying criteria and supporting information. (Note: Criteria, Evidence, Verification/Validation Method; and Reference Standard/Guidance should be understood to be illustrative examples only.)

TABLE 2 - SAMPLE USE CASE: OUTSOURCED SERVICE FOR MISSION CRITICAL FUNCTION

CRITERIA	EVIDENCE	VERIFICATION / VALIDATION	REFERENCE STANDARD / GUIDANCE
Bidder must have a continuity plan that ensures capability to recover within the required timeframe	Continuity Plan	3rd Party Review or QL Program Activity Review; Continuity Tabletop Exercise or Real-Life Continuity Event Results	Federal Continuity Directive 1 and 2 (or equivalent

Justification: The Government relies upon an outsourced service for the sustained performance of a mission critical function. To ensure continuity of operations, any disruption or failure of this function must be fully recoverable within 12 hours or less.

TABLE 3 - SAMPLE USE CASE: CLOUD SERVICE PROVISION OF SERVICE

CRITERIA	EVIDENCE	VERIFICATION / VALIDATION	REFERENCE STANDARD / GUIDANCE
Capability to Sustain Minimal Staffing Levels of Vetted, Qualified Personnel at Primary and Back-up Data Centers	Staffing Plan; Key Personnel Resumes; Vetting Requirements and Processes	Third Party/Qualified Program Activity Review	As determined by the Qualification Program Activity
Alternate Power Generation	Pictures; Documentation	On-site Verification; Bidder Certification; Third Party/Qualified Program Activity Review	Alternate Power Generation Equipment shall be of sufficient capability and Fuel Source must be on-site or demonstrated to be readily attainable.
Redundant Telecommunications	Documentation	Third Party/Qualified Program Activity Review	Redundant Telecommunications Services, of sufficient capacity must be in place and sustained and acquired from an alternate provider, unless this is not a verifiably available option.

Back-Up Data Centers are geographically dispersed, rely upon a separate part of the Energy Grid	Pictures; Documentation; Risk Assessment Used to Inform Location of Facilities	On-site Verification; Bidder Certification; Third Party/Qualified Program Activity Review	Data Centers shall be diversely located to mitigate against all potential natural risks (e.g., seismic, flood, fire, hurricane, etc.)

Justification: Bidder provides a Cloud Service Solution that is relied upon for multiple agencies of the Government and must be continuously available 24/7.

The WG3 report also built out summaries of the benefits and potential risks of Qualified Lists, as can be identified in Table 4.

TABLE 4 - SUMMARY OF BENEFITS, COSTS, AND RISKS ASSOCIATED WITH QUALIFIED LISTS

BENEFITS
Provides for a means to readily identify which entity(ies), product(s), or service(s) have been shown by an organization to satisfy a set of criteria, saving time and resources that would otherwise be spent evaluating against those criteria on a project by project basis.
Promotes use of standards.
Greater assurance that experienced, qualified personnel perform assessments, and do so in a consistent and fair manner.
When done well, qualification requirements and processes allow for more of a life-cycle focus vs. “point in time”.
Transparency about qualification is enabled by ensuring there is documentation about, and access to, the qualified list, and information about Q-list purpose, requirements, process steps, timeframes, and qualification-associated costs
Enables a more streamlined or accelerated procurement process. Concentrates and optimizes the use of resources involved in conducting an assessment
Allows for a means to selectively “raise the bar” vs. taking a one-size-fits-all approach (e.g., Q-list for CDM tool providers vs. applying same criteria and evidentiary requirements for *all* ICT tool providers)
Reduction in burden to industry by establishing common, standards-based requirements that reduces need to respond to duplicative, and potentially conflicting, requirements
COSTS & RISKS
Criteria must be tailored carefully to the security and functional objectives of those relying on the list or will lead to unintentional assumption of risk. Lack of clarity and understanding regarding the objective of the list and criteria considered can engender a false sense of security among list users.
Requires significant investment of resources (time, money, expertise) to build and maintain.
Failure to build and manage lists appropriately can expose those relying on the list to security vulnerabilities, lack of availability or logistical capability, legal liability, or other risks.
Geopolitical qualification criteria could lead to adverse reaction by other governments
A proliferation of separate QLs in any given area may make pose difficulties for entities seeking qualification, especially if the evaluation criteria and qualification methods are disparate

Establishing a qualified list requires balancing the need for such a list against the feasibility of establishing and maintaining such a list in a manner that is practical and sustainable. This includes considerations relating to governance of the list, those relating to qualification of covered articles or entities to be included on the list, and those relating to the handling of not-qualified or dis-qualified (adverse) decisions about applicants to the list.

CONCLUSION

WG3's materials can be found through the CISA website (http://www.cisa.gov/supply-chain). WG3's report provides valuable support material for encouraging introduction of its evaluation criteria into decision-making and planning around the development, structure, and utilization of QBL/QMLs.

WG3 continues to work with Task Force leadership to identify potential opportunities for continuing or new efforts. WG3 identified potential resources and opportunities to help support ICT purchase or utilization decision-making in the future and will work to evaluate opportunities within these areas.

SECTION VI — WORKING GROUP 4: VENDOR SCRM TEMPLATE

The Vendor SCRM Template Working Group (hereinafter WG4) created a standardized template of questions as a means to communicate ICT supply chain risk posture and analyze comparative risk among all types and sizes of organizations, to enable increased transparency in managing ICT outsourcing risks. These questions provide enhanced visibility into trust and assurance of the entity to assist in informed decision making about whether a business relationship introduces risk exposure at an acceptable level.

The purpose of the template is to standardize a set of questions regarding an entity's implementation and application of industry standards and best practices so that both ICT vendors and customers can coalesce on a way to communicate and understand that is more consistently understood, predictable and actionable, and addresses gaps in risk management. These questions are consistent with commercial and public sector standards. This enhances visibility by providing a flexible template that can help guide planning or assessments and provide clarity for reporting and vetting processes. It is meant to be non-prescriptive and no specific use case is being mandated.

The template is also meant to be agile. Questions can be recommended and aligned to categories; the ultimate user of the report (e.g., procurers of hardware, software, and services) can decide which questions to include based on the level of assurance required. The agility and flexibility also improve the utility of the template, ensuring it can be deployed to help stakeholders at a wide range of companies meet their particular concerns or needs.

The template can be found on the CISA website (www.cisa.gov/supply-chain).

GOAL AND OBJECTIVES

WG4 set out to address gaps in risk management and visibility by providing its vendor SCRM template as a flexible resource that can help guide planning or assessments. The template would provide clarity for reporting and vetting processes, helping acquisition professionals and staff purchasing ICT hardware, software, and services better understand and conduct their SCRM practices.

WG4 intended that its model and corresponding resources would be valuable for all stakeholders in the SCRM space, helping inform private-sector-to-private-sector interactions, as well as governmental requests for information from the private sector.

GOAL

WG4 defined its goal as helping make industry standards and best practices more consistent, predictable, and actionable. Working with best practices, including, but not limited to NIST security standards and risk guidelines, WG4 aimed to create a template for describing an ICT supplier's SCRM practices. This template would leverage existing tools and resources, including NIST SP 800-161 and ISO standards, along with building on the work of the other ICT SCRM Task Force working groups.

OBJECTIVES

WG4 was created to develop recommendations on a model or template for analyzing, implementing, and monitoring supplier or vendor SCRM practices. WG4 worked to create a template that could describe SCRM areas that are important for how federal agencies and private sector entities will evaluate ICT suppliers' supply chain assurance efforts.

WG4 set out to develop recommendations to help vendors and customers implement, incorporate, and utilize existing requirements relating to attestation, such as NIST standards. WG4's objective was to address gaps in risk management by providing a flexible framework that would serve as a planning resource by helping standardize and clarify reporting and vetting processes. The template is intended to provide that framework, encouraging its utilization in planning, reviewing, and clarifying risk reporting and supply chain vetting processes.

One critical element for WG4 was ensuring the template had the flexibility necessary to be used by a wide range of ICT stakeholders. SCRM concerns are not limited to companies of one size, and WG4 wanted to ensure that its product would be useful for both major ICT companies and for small- and medium-sized businesses. Some questions in the template would be more useful than others for stakeholders of various sizes, but the final product would provide value and utility for the widest possible range of stakeholders.

LINKAGE WITH OTHER EFFORTS

WG4 set out to ensure its work would be a valuable asset in informing the Task Force's interactions with other attestation and modeling efforts, including NIST SP 800-161, the Enduring Security Framework (Outsourcing Network Services Assessment Tool (ONSAT)), and the Department of Defense Cybersecurity Maturity Model Certification (CMMC) process and development. WG4 viewed its work as distinguishable from, but complementary to, the CMMC's approach to data and the specific areas of focus that it has been deploying and sharing publicly. WG4 intended that its model would be able to incorporate identified needs for addressing emerging issues, including software transparency.

OUTPUTS

WG4, working in tandem with the other Working Groups, built out its final template product to be a resource for ICT stakeholders and to help improve vendor SCRM compliance decision-making and awareness.

DELIVERABLES

WG4 developed a template that builds upon existing industry standards to provide step-by-step guidance and improved awareness. The template is a standard framework that helps users identify relevant categories of SCRM compliance and walks through key questions that can be used to inform SCRM security and resilience discussions or implementation.

WG4's template defines the categories of vendor SCRM compliance, building on a framework of key industry standards. The WG4 template, building on other Task Force efforts, incorporates inputs from key industry standards and best practices, including NIST SP 800-161 and the ONSAT tool. In shaping its categories, WG4 took the four supply chain threats from NIST SP 800-161 (security, integrity, resilience, and quality) and mapped them against the control categories defined by WG3 as part of its work.

TABLE 5 - THREAT CONTROL CATEGORIES ALIGNED TO NIST 800-161 SUPPLY CHAIN THREATS

SECURITY	INTEGRITY	RESILIENCE	QUALITY
Physical Security	Counterfeit prevention and detection	Resilience	Supply Chain governance and control
Cybersecurity	Product Tampering		Secure hardware & software product design and development
Protecting CUI			
Personnel Security			
Transparency of Ownership & Suppliers			

Using that as a baseline, WG4 evaluated the categories defined in the ONSAT tool and mapped them against the outputs of the WG3 definitional structure. WG4's mapping, aligned against the 4 categories from NIST SP 800-161, produced the category structure that is the framework of the WG4 template.

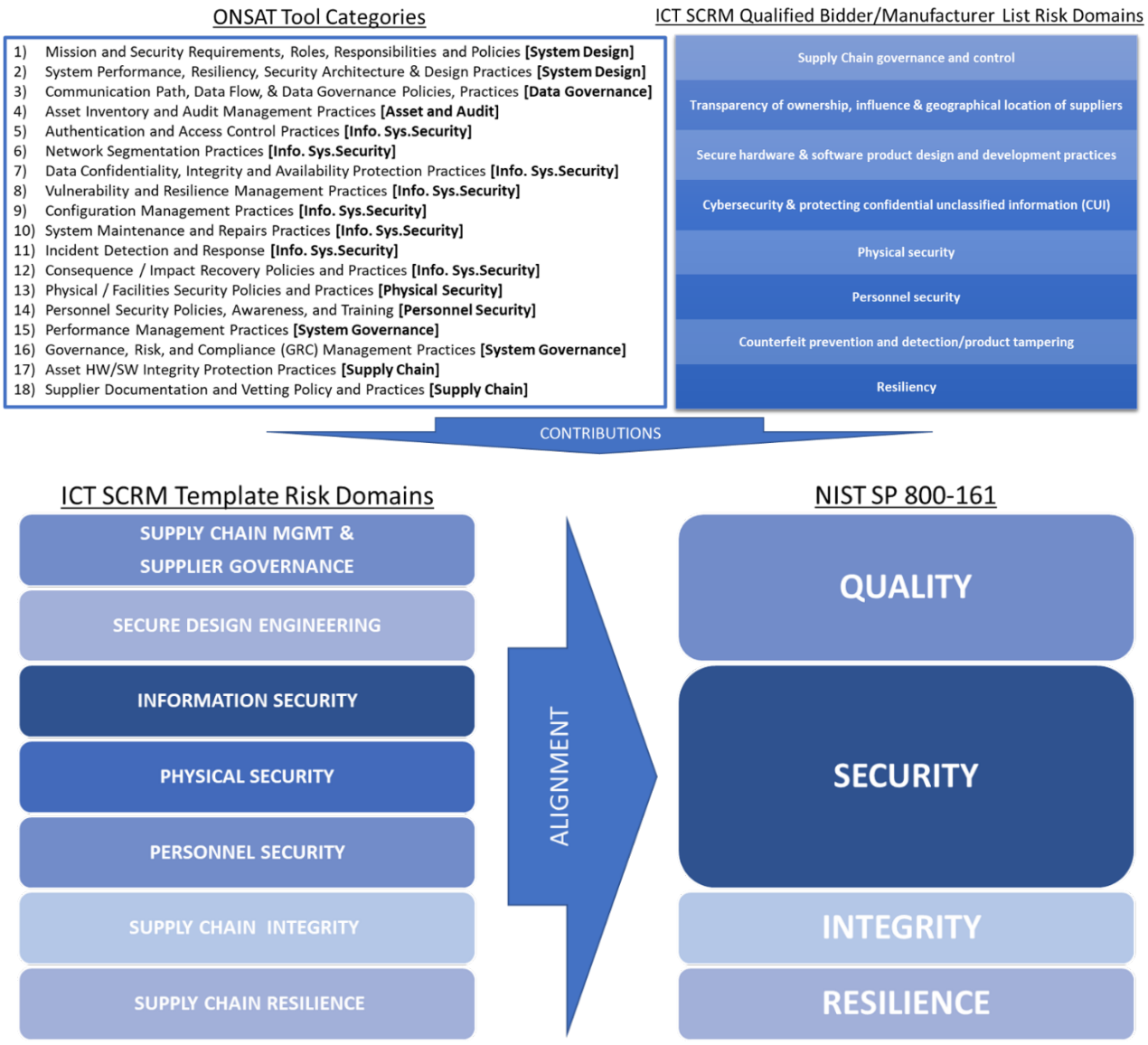

FIGURE 3 - WG 4 USED THE ONSAT TOOL CATEGORIES AND THE FRAMEWORK FROM WG3'S MAPPING OF NIST 800-161 TO DEFINE ITS CATEGORIES

With the category structure in place, WG4 began to build out the content to populate the framework and provide the actionable measures for the template. Within each category, the template includes questions and sub-questions for each category to support the operationalization and utilization of the template. The questions were broken down into three levels:

- Level 1: Answerable with "Yes," "No," "N/A," or "Alternate Response"
- Level 2: Respondent describes what satisfies the requirements.
- Level 3: Respondent describes how it satisfies the requirements."

By defining the three categories of questions, WG4 was able to ensure greater flexibility for the template and shape areas where additional detail or strict compliance requirements would better serve evaluations of SCRM security and resilience. Table 6 highlights examples of questions prepared by WG4.

TABLE 6 - EXAMPLE QUESTIONS APPEARING ON THE WG4 TEMPLATE

INFORMATION SECURITY CATEGORY SAMPLE QUESTIONS
4. Information Security 4.1. Do you hold a valid information security/cybersecurity third party attestation or certification? (e.g. ISO 27001, SOC 2 Type 2, CMMC Level 3-5, Cybersecurity Maturity Assessment, etc.) **[If yes, please state the program that certified you and date of last certification. Please provide a copy. You may skip the remaining questions of this section and proceed to the following section. If not, continue.]**
4.2. Do you follow operational standards or frameworks for managing Information Security/Cyber security? (e.g., NIST CSF 1.1, NIST 800-37, Rev. 2, NIST SP 800-161, ISO IEC 27001, ISO 20243, ISO 27036, SAE AS649) [Yes, No, Alternate, or N/A] 4.2.1. If so, which one(s)? Please provide. 4.3. Do you have company-wide, publicly available Information Security policies in place covering Privacy policies? [Yes, No, Alternate, or N/A] 4.3.1. If 'Yes', please provide. 4.3.2. What mechanisms are in place to ensure your policies are enforced within your supply chain? 4.3.2.1. Do you receive notification of and have a response plan in place for privacy violations of the suppliers in your supply chain?

The opening question of this section highlights the flexible approach the template provides. While it is slightly out of the standard format, it provides the ability to bypass certain questions if an adequate response can be provided in the initial question. The ability to customize and potentially shorten the questionnaire will facilitate adoption by reducing potential resourcing needs and allowing it to better fit the specific circumstances of some stakeholders.

LINKS TO OTHER ICT SCRM TASK FORCE WORKING GROUPS

WG4 worked to align its work with that of the other ICT SCRM Task Force Working Groups, utilizing the Task Force's cohesive approach to maximize its effectiveness. WG4 grounded its work in the work being completed by WG3, defining its seven categories of questions to align to the WG3 framework (see Section V). WG3 had mapped the NIST SP 800-161 standards to its initial categories, providing an initial basis for WG4 in developing and aligning its categories.

TABLE 7- WORKING GROUP 4 ALIGNED THE CATEGORIES FOR ITS TEMPLATE TO THE CATEGORIES DEFINED BY WORKING GROUP 3

WORKING GROUP 3 CATEGORY	WORKING GROUP 4 CATEGORY
Physical Security	Physical Security
Cybersecurity	Cybersecurity
Personnel Security	Personnel Security
Hardware Integrity	Supply Chain Integrity
Software Integrity	Supply Chain Integrity
Supply Chain Resilience	Supply Chain Resilience

Supply Chain Management & Supplier Governance	Supply Chain Management & Supplier Governance
Secure Design Engineering	Secure Design Engineering

In creating the template, WG4 also leveraged the information collected as part of the inventory of supply chain-related standards conducted during Year 1 of the Task Force. Access to this look at the relevant standards helped align the final product to existing frameworks, ensuring it would be more accurate, more useful, and more easily incorporated with ongoing efforts.

CONCLUSION

WG4 is finalizing its product that has the necessary flexibility to ensure its utility for stakeholders throughout the critical infrastructure space, regardless of the size or complexity of the company. Its products will be found on the CISA website (www.cisa.gov/supply-chain). The Template and supporting products will provide the key questions, metrics, and measures that can be used to inform SCRM security and resilience discussions. Within each category, the template includes questions and three levels of sub-questions to support the implementation and utilization of the template. These questions will help vendors and customers communicate in a way that is more consistently understood, predictable and actionable.

The Task Force is discussing options for potential future efforts relating to other objectives or utilization of the WG4 template, including integration into a platform that allows greater interactivity and broader utilization.

SECTION VII — WORKING GROUP 5: COVID-19 RISK STUDY

The ICT SCRM Task Force established the COVID-19 Supply Chain Risk Analysis Study Working Group (hereafter, WG5) in response to the 2020 COVID-19 pandemic. WG5 analyzed the impacts from COVID-19 on ICT supply chains, particularly as it relates to supply chain resiliency, to avoid more serious impacts during potential future events.

WG5's report, including visualizations and mapping efforts supporting the SCRM environment and possible "chokepoints," can be found on the CISA website (www.cisa.gov/supply-chain).

GOAL AND OBJECTIVES

WG5 sought to understand and analyze the impacts from COVID-19 on ICT supply chains. The goal of this analysis was to stimulate public awareness and dialogue on ICT supply chain considerations and develop practical recommendations that ICT stakeholders can use to enhance their supply chain resiliency efforts. The study of lessons learned enables a shared understanding between policy makers and ICT-centric organizations on the opportunities to make more resilient risk management decisions in the future that enhance supply chain resiliency outcomes.

OBJECTIVES

WG5 worked to identify the impacts on ICT supply chains due to COVID-19. By understanding supply chain impacts, organizations can create enhanced resiliency for their supply chains in the future. This study will assist the ICT SCRM community in creating a shared understanding of the impacts to the ICT supply chain due to the pandemic.

OUTPUTS

The WG5 Study analyzed the impacts to the ICT supply chains during the pandemic. It focused on three main themes: inventory management, supply chain transparency, and single-source and single-region suppliers. The study also produced a high-level visual mapping of how goods and services flow through the generalized ICT supply chain, from the raw materials stage through to sale to the customer. The map also identifies examples of chokepoints that can occur throughout the supply chain.

IMPACT STUDY

WG5 completed the study in partnership with private sector and industry associates to facilitate the collection of first-hand data from ICT supply chain companies. The group created and disseminated an electronic question set to industry partners and trade associations to obtain information on how the pandemic impacted their supply chains. As a part of the study, WG5 created a supply chain system map that visualizes the ICT supply chain routes, from source material to end user consumption, and identifies chokepoints and vulnerabilities that impact the supply chain.

As part of that study, WG5 identified three major stress points on ICT supply chains during the pandemic:

- The pandemic exposed how some manufacturing companies were unprepared because of their reliance on lean inventory models, which provide great efficiency and cost effectiveness in normal environments
- COVID-19 underscored the difficulties that companies face in understanding their junior tier suppliers and where they are located
- The pandemic underscored the need for an approach that was already underway over the last six years: diversifying supply chains to a broader array of locations and away from single source/single region suppliers

WG5 conducted further evaluation of these three components by linking them to additional studies on supply chain disruptions, lessons learned from past disruptions, and key insights from analysis of the pandemic-induced disruptions.

Inventory Management

The typical approach to supply chain management emphasized the need to strike a balance between efficiency and resiliency. While these concepts are often at odds with one another, effective supply chains strike the right balance between the two. Increased competition and often-compressed profit margins have driven supply chain managers to emphasize cost reduction, just in time deliverables (JIT), and days of supply inventory management. While lean supply chains may work in times of normalcy, the pandemic has demonstrated that companies may need to examine their current inventory management practices so that they can continuously collect data and feedback, evaluate it continuously, react expeditiously to rapidly evolving environments and develop cushions to absorb abnormal periods of activity or inactivity.

Supply Chain Transparency

During the COVID-19 pandemic, many companies worldwide rushed to ascertain which of their "invisible" junior-tier suppliers—those with whom they do not deal with directly—were based in the affected regions that experienced shutdowns, disruptions to work and transportation, and access to supplies. To create supply chain resilience, managers need the ability to map where their Tier 1, Tier 2, and Tier 3 suppliers are located so they can understand which suppliers are most affected by disruptions. They also need visibility into tracking junior suppliers' inventory of finished goods and raw materials.

Single-Source and Single-Region Suppliers

In many cases, companies struggle with their reliance on a single source for products that they purchase directly. While supply chain managers recognize the risk of an over-reliance on a single source, some may nevertheless adopt this strategy to secure the necessary supply or to control costs. This lack of redundancy can have significant effects when a company's sole supplier goes down. ICT supply chain companies often have limited options for sourcing certain materials, or it may have sourcing options only from a single region, continent, or company.

SUPPLY CHAIN MAPPING EXERCISE

WG5 provides a high-level visual mapping of how goods and services flow through the generalized ICT supply chain, from the raw materials stage through to sale to the consumer. The map identifies the chokepoints that can occur throughout the supply chain. This type of initial mapping exercise illustrates the importance of mapping efforts in building transparency and common understanding into the supply chain risk management process, as it is useful in identifying hidden relationships that can impact resiliency. The high-level visualizations created by WG5, specifically looking at transportation and production chokepoints, illustrates the relationships and process flows that need to be explored in supporting these efforts.

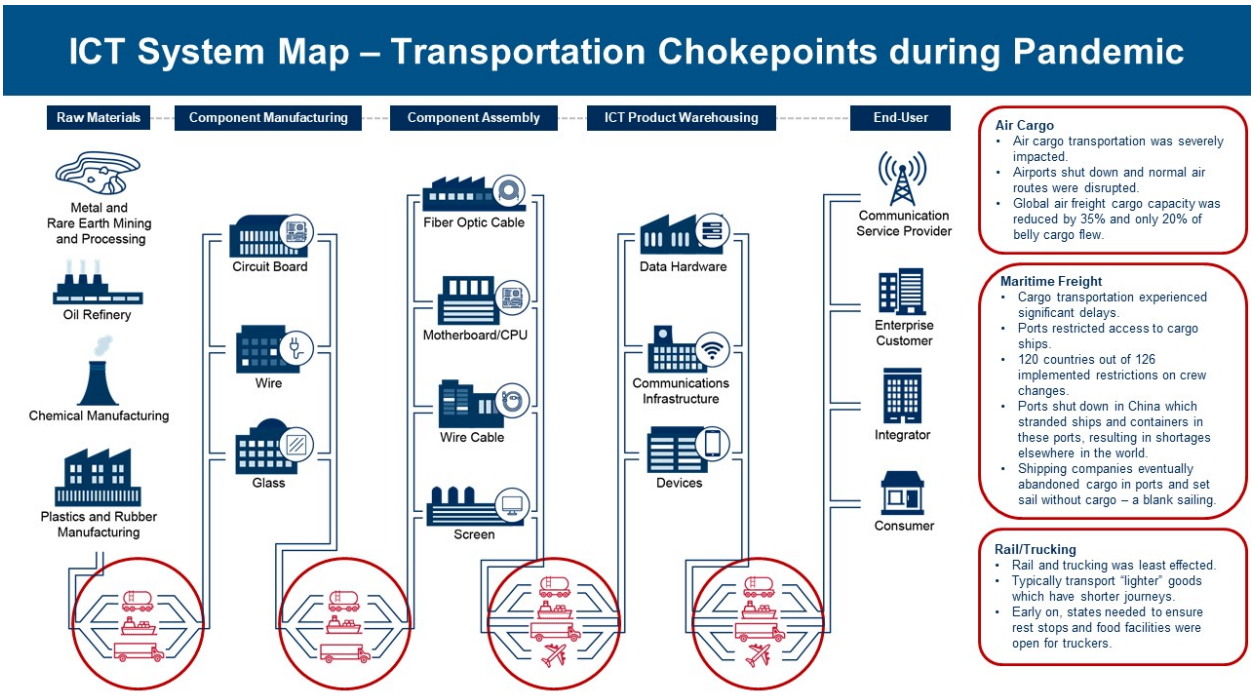

FIGURE 4 - WORKING GROUP 5 IDENTIFIED THE TRANSPORTATION CHOKEPOINTS IN ITS AN ICT SUPPLY CHAIN MAP

Correspondingly, in the mapping of the Production chokepoints, WG5 identified that chokepoints fell into 5 major categories:

- **Manufacturing Delays:** There were across the board manufacturing slowdowns in all tiers of the supply chain, including difficulty acquiring supplies to manufacture key components and an increase in lead-times
- **Cross-border Inconsistency:** Other nations had different definitions of essential factory workers than the U.S., resulting in factory shutdowns; even within the US, states and municipalities used different definitions
- **Supplier Communication:** There was difficulty reaching manufacturers for weeks after the pandemic struck and factories were shuttered, with communications challenges particularly apparent for Tier 2 suppliers and those below
- **Supplier Transparency:** There was a lack of visibility of who suppliers are below Tier 1 and where they are located, with suppliers often demonstrating an unwillingness to share sourcing information such as Bill of Materials, inhibiting risk understanding
- **Customer Order Delays:** Manufacturing and shipping delays resulted in order fulfillment delays for customers

RECOMMENDATIONS

WG5 developed recommendations based on its analysis and discussions with a range of ICT stakeholders, gearing its recommendations to be applicable at both large and small companies. These practical recommendations look at opportunities to build additional resilience into ICT supply chains in the future, working to support policy and operational decisions to strengthen supply chains going forward. Those recommendations landed in the following categories:

- Considering Proactive Risk Classification
- Mapping the Corporate Supply Chain
- Broadening Supplier Networks and Regional Footprints
- Potentially Developing Standardized Mapping and Illumination Tools

- Exploring Shifts in Optimizing Inventory Practices
- Planning Alternatives in Logistics and Transportation

CONCLUSION

The ongoing impacts of the COVID-19 pandemic on the ICT supply chain are still unfolding, and potential shifts in supply chain risk identification, management, and mitigation may shape the ICT supply chain well into the future.

WG5 completed its study and presented the findings to the ICT community where they were well-received. The study's recommendations can assist the ICT industry in building enhanced resiliency in their supply chains going forward. Visit the CISA website (www.cisa.gov/supply-chain) to see the completed study, along with sample mapping and the underlying recommendations.

SECTION VIII — FUTURE OF THE ICT SCRM TASK FORCE

The ICT SCRM Task Force is a center of gravity for industry-government collaboration. The unique perspectives its members provide help address emerging and evolving challenges in the ICT supply chain environment. Two years ago, the Task Force set out to use this connection between government and industry partners to develop actionable recommendations, partnerships, and activities geared toward improving supply chain security and resilience. As the Task Force moves into its third year, it will build on its prior successes and strengthen the partnership structure to more effectively manage the evolving threat environment.

The Task Force will continue to identify options for maximizing implementation and impact of its work, with a focus on efforts to operationalize recommendations and transition them to use. The Task Force's efforts have improved the understanding of, capability for, and design of security and resilience measures, and, in Year 3, the Task Force is positioned to build on those successes and drive additional positive future outcomes. The Task Force can, utilizing coordination links it developed and strengthened, develop proactive measures for influencing security and resilience decision-making throughout the decision lifecycle.

For example, the Task Force's Coordination Tiger Team developed an inventory of relevant supply chain related authorities, programs, and areas of interest, improving the collective understanding of how the various elements of the supply chain risk management environment work together. In Year 3, the Task Force can leverage these mapping and partnership building efforts to improve prioritization and coordination throughout the ICT supply chain environment, driving increased identification, utilization, and effectiveness of security and resilience measures. The Task Force has shown that it ensures better linkages between industry and relevant government efforts, including the FASC. In Year 3, the Task Force will continue to bolster these connections, ensuring perspectives and expertise from across sectors and government are reflected in these efforts.

The Task Force members will continue to bring their unique capabilities to develop advice and engagement activities that provide actionable, scalable solutions for supply chain challenges. The Task Force will continue to grow, where appropriate, its engagement with relevant critical infrastructure sectors and stakeholders, working with its sector partner and international partners in the coming year to identify opportunities for expanding, honing, expanding, and utilizing the Task Force's work and its expertise. One critical element of the Task Force's Year 3 work will be working with its relevant partners across government, industry, and new partners to leverage the necessary expertise for translating the Task Force's successes into measurable impacts.

As it moves into Year 3, the Task Force will continue to leverage its collaborative process to identify the relevant opportunities for new efforts, emerging issues, or shifts in its structures to address needs of the Task Force, its membership, and its stakeholder partners.

SECTION IX — CONCLUSION

We live in a system of systems world where ICT components underpin a broad range of critical infrastructure and governmental functions the American people depend upon. The ICT SCRM Task Force is an invaluable resource in supporting collaboration between government and industry to address the ever-changing threat and operational landscape. Over its first two years of operation, the Task Force demonstrated its ability to successfully leverage engagements and deploy its collective expertise to advance the cause of security and resilience of ICT systems and components.

The Task Force completed and will continue to provide valuable products, tools, resources, and analysis to help support a wide range of ICT SCRM decision-making and planning efforts. Content developed by the Task Force can be found on the CISA website at www.cisa.gov/supply-chain, with specific Task Force documents on www.cisa.gov/ict-scrm-task-force.

The CISA supply chain website is also a useful source of other graphics, resources, and products from CISA, including:

- Work from Year 1 of the Task Force
- An ICT Supply Chain Risks infographic
- A Supply Chain Risk Management Essentials guide for leaders and staff with actionable steps on how to start implementing organizational SCRM practices
- An Internet of Things (IoT) Acquisition Guidance document
- Reports, infographics, and other materials related to introduction of 5G technology in the United States

Despite facing unforeseen and unprecedented challenges in 2020, the ICT SCRM Task Force continued to successfully build on its prior efforts, tackle pressing challenges, and position its participants to provide the flexibility, expertise, and collaboration needed to build a more secure and resilient future. The Task Force looks forward to working with members and partners to meet the changing ICT SCRM environment and identify where it can most effectively support critical SCRM efforts.

The Cybersecurity and Infrastructure Security Agency's (CISA) National Risk Management Center (NRMC) is the planning, analysis, and collaboration center working in close coordination with the critical infrastructure community to Identify; Analyze; Prioritize; and Manage the most strategic risks to National Critical Functions. These are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof. NRMC products are visible to authorized users at HSIN-CI and Intelink. For more information, contact NRMC@hq.dhs.gov or visit https://www.cisa.gov/national-risk-management.

APPENDIX A — DEFINITIONS

TERM	DEFINITION
5G	Fifth generation mobile network, whose specification the International Telecommunication Union (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). (Source: Newton, Harry, Steve Schoen, Gail Saari, and Leigh McLellan. *Newtons Telecom Dictionary*. New York: Harry Newton, 2018.)
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.
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. (Source: Presidential Policy Directive 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. (Source: CIPAC Frequently Asked Questions)
Federal Acquisition Security Council (FASC)	An interagency council, chaired by the Office of Management and Budget (OMB), with authorities and functions described in subchapter III of chapter 13 of Title 41, United States Code. The Council's functions include 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. (Source: SECURE Technology Act, P.L. 115-390, Title II (Federal Acquisition Supply Chain Security Act of 2018); 41 U.S.C. § 1321-28.)
Information and Communications Technology (ICT)	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. (Source: International Telecommunication Union)
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. (Source: National Institute of Standards and Technology)

TERM	DEFINITION
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. (Source: 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 constitutes all forms of intentional, unintentional, accidental, incidental, misuse, abuse, error, weakness, defect, fault, and/or failure events and associated conditions. (Source: NIST SP 800-161)
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. (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. (Source: 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. (Source: 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. (Source: Software and Supply Chain Assurance Forum)

APPENDIX B — EXECUTIVE LITIGATION RISK AWARENESS MATRIX

Informed by group discussions, the private sector members of Working Group 1, in conjunction with Federal subject matter experts, developed the following matrix as a decision support tool to support ongoing conversation relating to information sharing. This matrix does not constitute legal advice, nor does it reflect the policy of the federal government. Rather, it was developed by members of Working Group 1 as a mechanism for illustrating potential approaches relating to mitigating litigation risk. The matrix is below.

There are three general categories of possible allegations that could be the basis of claims in private litigation. For present purposes we treat the litigation risk of each category as the same, although different facts could make one type of claim more likely (e.g., breach of confidentiality claims more likely in the presence of a contractual relationship between plaintiff and defendant):

- **Anti-competitive behavior:** ECONOMIC or BUSINESS TORT CLAIMS (e.g. Interference with Business Advantage)
- **False information:** DEFAMATION or MISREPRESENTION TYPES OF CLAIMS (e.g. Business Defamation, Trade Libel, Fraud)
- **Breach of obligations of confidentiality:** TRADE SECRET CLAIMS and BREACH OF CONTRACT (e.g., revealing practices, processes, designs, etc. that the manufacturer may assert are protected trade secrets, breach of express nondisclosure language in a quote, contract, etc.)

PRIVATE LITIGATION RISK SPECTRUM

Low: Suit would be dismissed.	**Medium:** Suit could survive motion to dismiss, reach discovery.	**High:** Suit could prevail.

High-level factors that move the reporting company along the spectrum of litigation risk*:

- Intent to serve the public interest… **vs…** Intent to harm the reported supplier or gain private benefit.
- Good faith belief in the veracity of the concern reported… **vs…** Spurious maligning of reported supplier.
- Degree of care in vetting the credibility of facts reported… **vs…** Careless innuendo and sharing rumors.

Type of concern	Low: Criminal activity (e.g., espionage, sabotage)	Low: Suspected criminal activity	Medium: Unethical business practices	Medium: Insecure hardware, software	High: Poor quality hardware, software
Level of certainty	Low: Facts confirmed with documentary evidence**	Low: Facts, sources heavily vetted, credible**	Medium: Facts credible, prelim. investigated**	High: Facts credible but not investigated	High: Unconfirmed rumor
Formality of reporting	Low: Filing under a statutory regime or similar model	Low: Signed statement also filed with LE/govt	Medium: Signed statement to one or more private parties	Medium: Oral report to one or more private parties	High: “Whisper campaign”
Audience of the reported concern,	Low: Contractual relationship, required reporting	Low: Group for sharing criminal or safety	Medium: Minimal commercial interest	High: Reporting party seeks business with	High: Reporting company has contractual

relationships between parties		supply chain concerns (inc. with LE/govt)	between reporting party and recipient	recipient, is competitor with reported supplier	relationship with reported supplier
Government's role	Low: Formal proceeding or government contract, required reporting	Low: Formal program with procedural steps for reporting	Medium: Express interest in private reporting	Medium: Implied interest in private reporting	High: No interest in private reporting
Message reported	Low: Anonymized	Low: Only name the country of concern	Medium: Use euphemisms for the supplier	Medium: Identify a class of companies	High: "Do not buy from this company!"

*Note that some of these factors may impact the amount to damages in addition to or instead of the veracity of the claim. This chart does not separately assign weight to the impact of these considerations on damages.

**Note that the truth of the reported concern is not a defense to breach of contract or misappropriation claims, but depending on the severity of the concern, a public policy defense may be available.