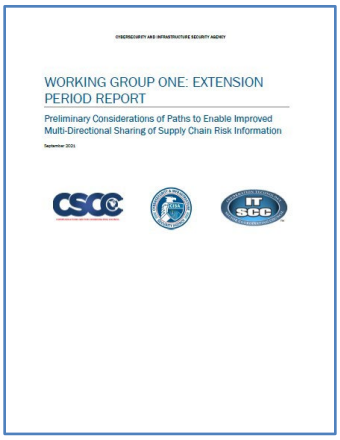
IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

SHARING SUPPLY CHAIN RISK INFORMATION TO INCREASE RESILIENCE

THE CHALLENGE OF INFORMATION SHARING



Improving the quality and volume of information sharing among the federal government and private industry is necessary to obtain actionable information that could mitigate threats to the Nation's information and communications technology (ICT) supply chain. Significant barriers to the sharing of supply chain risk information (SCRI) exist.

This report is the culmination of a multi-year effort by the Cybersecurity and Infrastructure Security Agency's (CISA) Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force to address the issues of sharing SCRI between companies and government entities. The initial work defined a common framework for the bi-directional sharing of actionable SCRI between federal government and industry.

Subject matter experts (SMEs) researched legal and policy considerations for private enterprise or government utilization in addressing liability limitations. The SMEs found that limiting liability would facilitate the most effective sharing of actionable SCRI with the government or between companies.

This report focused its research on paths to limit certain state law causes of action, to which a business may be exposed to by virtue of its sharing of SCRI. This report offers research by SMEs on legal and policy considerations to be used by private enterprises or government in seeking to address the issue of liability limitations. This report contains consensus input of non-federal members and does not reflect the official policy or position of the federal government or its official representatives.

THE IMPORTANCE OF INFORMATION SHARING

The report, titled Preliminary Considerations of Paths to Enable Improved Multi-Directional Sharing of Supply Chain Risk Information, details how the sharing of information on suspect suppliers SCRI between the federal government and industry is an important avenue in which to mitigate the threats to the nation's ICT supply chain. This body of work reflects the fact that private and public sector entities share the same global ICT supply chain and therefore share the same risks. All organizations that are part of this supply chain should be aware of these information sharing issues.

LIMITATIONS AND BARRIERS FOR SHARING SCRI

To improve the sharing of SCRI, including naming suspect suppliers, and to provide protection from potential liability for sharing information, this report recommends amending the 2015 Cybersecurity Information Sharing Act to specifically add supply chain risk as a form of information that constitutes a cyber threat indicator. If SCRI was explicitly listed as a class of information considered a cyber threat indicator, entities would have clear legal authority to share SCRI in accordance with the statute without fear of litigation.

The report offers SME research on legal and policy considerations for providing liability protection to the private sector to promote information sharing about suspect suppliers. In developing the report, seven potential causes of action that could impose significant liability on private entities for sharing supply chain risk information are considered:

- Tortious Interference, Existing Contract
- Tortious Interference, Prospective Contract
- Business Relationship or Business Advantage
- Business or Commercial Disparagement

- Defamation
- Breach of Contract
- Misappropriation of Trade Secrets

Below is an excerpt from the report's appendix showing causes of action and the mitigating factors as well as corresponding safe harbor solutions for sharing SCRI.

Table 1: Potential Standard for SCRI Sharing with Private Party or Government Based on Identified Causes of Action

Cause of Action	Mitigating Factors	Proposed Corresponding Solution of Safe Harbor
Tortious Interference with Existing Contract	▪ Lack of improper motive ▪ Truth of allegation ▪ Good faith basis for allegation (some jurisdictions) ▪ Degree of diligence undertaken (some jurisdictions) ▪ Legitimacy of business purpose (some jurisdictions) ▪ Whether disclosure was prompted by law, contract, or government request (some jurisdictions) ▪ Lack of damages	▪ Provide that Business A may share SCRI to Business B to further a legitimate purpose of protecting supply chains, improving supply chain security, and addressing supply chain vulnerabilities ▪ Create carve-out for existence of improper motive such that liability protection would no longer apply ▪ Include provision stating that Business A may legally share such information with Business B (including the Government) ▪ Require Business A to possess at least a medium level of confidence in the SCRI it shares
Fraudulent Misrepresentation	▪ Lack of intent to defraud ▪ Truth of information (i.e., no misrepresentation) ▪ Inability or difficulty showing reliance based on alleged misrepresentation	▪ Require Business A to possess a level of confidence in the SCRI it shares
Breach of Contract	▪ Disclosure for public policy purposes may be defensible	▪ Consider provision stating that SCRI demonstrating a high degree of risk (or that represents a violation of law) be legally mandated for disclosure to government to address potential

RESOURCES

- ICT Supply Chain Risk Management Task Force: CISA.gov/ict-scrm task-force
- Video on Improving Multi-Directional Sharing of Supply Chain Risk Information - YouTube