WORKING GROUP ONE: EXTENSION PERIOD REPORT

Preliminary Considerations of Paths to Enable Improved Multi-Directional Sharing of Supply Chain Risk Information

September 2021

This page is intentionally left blank.

WORKING GROUP ONE: EXTENSION PERIOD REPORT

Preliminary Considerations for Paths to Enable Improved Information Sharing

Executive Summary

The purpose of this report is to offer subject matter expert research on legal and policy considerations for private enterprise or government utilization in addressing liability limitations. It was determined that limiting private companies' and government liability would facilitate the most effective sharing of supply chain risk information (SCRI) with the government or between companies. Improving the omni-directional supply chain threat 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. The report was provided to the government as the consensus input of non-Federal members and does not reflect the official policy or position of the Federal government or its official representatives.

INFORMATION SHARING WORKING GROUP 1 (WG1) MEMBERS

Leadership team for WG1:

	Name	Company
Co-Chair	Cherylene Caddy	Department of Energy
Co-Chair	Edna Conway	Microsoft
Co-Chair	Joyce Corell	Office of Director of National Intelligence
Co-Chair	Kathryn Condello	Lumen

WG1 consists of the following members:

Agency	Company
Cybersecurity and Infrastructure Security Agency	AT&T
Department of Energy	Cellular Telecommunications and Internet Association
Department of Justice	Dell
Department of Treasury	FireEye
Federal Communications Commission	IBM
Federal Energy Regulatory Commission	Information Technology Industry Council
Office of Director of National Intelligence	Lumen
	Microsoft
	NTCA – The Rural Broadband Association
	Synopsys
	T-Mobile
	Telecommunications Industry Association
	Venable
	Wilkinson Barker Knauer Law

OVERVIEW OF REPORT

Working Group One (WG1) of the Cybersecurity and Infrastructure Security Agency's (CISA) Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force has determined that omni-directional supply chain threat information sharing among the federal government and industry is necessary to obtain actionable information that could mitigate threats to the nation's ICT supply chain. A group of non-federal subject matter experts convened to advise the U.S. government and concluded that the most effective means to facilitate sharing supply chain risk information (SCRI) by a private company (Business A) with another private company or the U.S. Government (collectively Business B) concerning a third-party company (Business C) would be to limit the legal liabilities of the sharing entity (Business A).

Our goal in this six-month extension period was to focus research on paths to limit certain state law causes of action to which Business A may be exposed by virtue of its sharing of SCRI. This report offers research by subject matter experts on legal and policy considerations to be utilized by private enterprises or government in seeking to address the issue of liability limitations. This report is provided to the government as the consensus input of the non-federal members of WG1 and does not reflect the official policy or position of the federal government or its official representatives.

WG1 assessed two questions:

> (1) for the purposes of an SCRI sharing framework, how is SCRI defined; and
>
> (2) what due diligence parameters must be met to gain the benefit of liability protections?

This report:

- Offers for consideration including identify supply chain risk as defined in 50 U.S.C. § 2786(e)(6)[i] , suggesting an additional subparagraph to the definition of Cyber Threat Indicator in Section 102 (6) of the 2015 Cybersecurity Information Sharing Act, hereinafter referred to as CISA 2015 (CISA 2015) and
- Provides key considerations including due diligence parameters that could be reflected in potential legislation to reduce liability in the SCRI-sharing context

PROPOSED ADDITION TO CISA 2015

To support the Task Force's goal of improving the sharing of SCRI, (to include naming names of suspect suppliers) and to provide protection for such information sharing from potential liability, this report offers for consideration the amending of CISA 2015 to specifically add supply chain risk as a form of information that constitutes a Cyber Threat Indicator. WG1 offers as an example for consideration the addition of simple language shown below in parts (H) and (I) and italics text to achieve this change:

> (6) Cyber Threat Indicator—The term cyber threat indicator means information that is necessary to describe or identify:
>
> > (A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability
> >
> > (B) a method of defeating a security control or exploitation of a security vulnerability

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability

(E) malicious cyber command and control

(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat

(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law

(H) supply chain risk, as described in 50 U.S.C. § 2786(e)(6) or

(I) any combination of 6(A) through 6(H).

WG1 offers for consideration, leveraging a definition of the term supply chain risk that already exists in U.S. law. Specifically, the definition from the chapter of the U.S. Code that governs atomic energy defense (50 U.S. Code § 2786, Enhanced procurement authority to manage supply chain risk) which states:

> **(e)(6) Supply chain risk** – The term supply chain risk means the risk that an adversary may sabotage, maliciously introduce an unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system or covered item of supply so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of the system or item of supply.

CISA 2015 provides authorization for sharing cyber threat indicators for the purpose of preventing, detecting, analyzing, and mitigating cybersecurity threats. 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.[ii] Among the many references and possible models for a SCRI sharing regime, the purpose and protections contained in CISA 2015 are offered as aligned with the goals identified by WG1. [iii]

KEY CONSIDERATIONS FOR REDUCING LIABILITY IN THE SCRI-SHARING CONTEXT

In the Year Two Report, WG1 considered seven potential causes of action that could impose significant liability upon private entities for the sharing of information, either with other private or public entities. Table 1 summarizes these causes of action and includes key mitigating factors.

TABLE 1—SUMMARY OF POTENTIAL INFORMATION SHARING CAUSES OF ACTION AND KEY MITIGATING FACTORS

CAUSE OF ACTION	KEY MITIGATING FACTORS
Tortious Interference with Existing Contract	▪ Motive behind interference ▪ Truth as a bar to liability ▪ Degree of diligence in ascertaining truth ▪ Passive versus active interference ▪ Legitimate Business Purpose defense ▪ Ability to invoke privilege
Tortious Interference with Prospective Contract, Business Relationship or Business Advantage	▪ Higher standard for establishing improper interference ▪ Higher standard for establishing likelihood of economic benefit ▪ Scope of audience disclosing to may affect liability ▪ Ability to invoke privilege
Defamation	▪ Truth of statement and degree of diligence undertaken in ascertaining truth ▪ Whether actual malice standard applies ▪ Plaintiff may not be required to prove damages if defamation *per se* ▪ Ability to invoke privilege ▪ Dissemination of information no greater than necessary ▪ Naming the plaintiff in the published statement not necessarily required, liability can attach by inference or ability for the plaintiff to be identified ▪ Some additional protections exist for disclosure to government but remains highly fact specific
Business or Commercial Disparagement	▪ Some overlapping considerations with defamation ▪ Intent to cause economic loss based on disparagement typically required (i.e., higher standard of intent than defamation) ▪ Plaintiff's burden to prove falsity ▪ Certain privileges may apply and would likely mirror defamation analysis (short of lack of bad faith) ▪ Proof of special damages required
Fraudulent Misrepresentation	▪ Higher pleading threshold ▪ Requirement to prove intent for another to change their position based on fraudulent representation ▪ Plaintiffs experience difficulty showing reliance on representation ▪ Fraudulent statements to a government entity could result in criminal as well as civil liability

	▪ Less factually aligned with circumstances concerning SCRI disclosure from Business A to Business B when evaluating exposure for a suit by Business C
Breach of Contract	▪ No intent element ▪ Simple pleading standard that focuses on disclosure of information ▪ Highly fact-dependent—what does the contract say? ▪ Public policy defense may be available ▪ Protections exist based on disclosure to government but remains fact specific
Misappropriation of Trade Secrets	▪ No intent element ▪ Statutory claim, not common law ▪ Breach of contract can be *prima facie* evidence of misappropriation ▪ Can occur in absence of legal relationship ▪ Plaintiffs have to prove many elements, which can be difficult ▪ Requires careful treatment of outside information and knowledge of sources ▪ Could have cascading liability through subsequent/downstream misappropriations caused by defendant ▪ Protections exist based on disclosure to government, but remains fact-specific ▪ If defendant did not have a right to the information in the first instance, it is less likely that a defense will apply

While the standards for many of the most likely causes of action are fact-specific, subjective, and jurisdiction-specific, Table 1 outlines various factors and criteria that could be memorialized in CISA to improve the existing protections under that statute, to better ensure protection for a company sharing SCRI. For ease of reference, Appendix A to this report reformats this information by causes of action. Please note that the below solutions are proposed as conceptual considerations and have yet to be reduced to specific statutory provisions or language.

Table 2 outlines some additional observations and general considerations that could inform any specific statutory provisions or language.

TABLE 2—STATUTORY PROTECTIONS FOR CONSIDERATION

PROPOSED STATUTORY AND RELATED CONSIDERATIONS	CAUSE OF ACTION ADDRESSED
Create specific legal authorization that Business A may share SCRI to Business B (or the Government) to further a legitimate purpose of protecting supply chains, improving supply chain security, and addressing supply chain vulnerabilities.	▪ Tortious Interference with Existing Contract ▪ Tortious Interference with Prospective Contract, Business Relationship or Business Advantage ▪ Defamation

PROPOSED STATUTORY AND RELATED CONSIDERATIONS	CAUSE OF ACTION ADDRESSED
Two approaches to what a legitimate purpose is exist. It can either be presumed or demonstrated via evidence by Company A. There are pros and cons of a presumption versus the need for Company A to demonstrate or evidence such.	▪ Business or Commercial Disparagement
Require Business A to possess at least a Medium level of confidence in the SCRI it shares as of the time of sharing such SCRI. Requiring Business A to possess a High level of confidence or complete certainty in the SCRI it shares would enable greater liability protections. Each enterprise or government member of the TF should consider whether it agrees with the confidence levels set out in CISA. [iv] [v] [vi]	▪ Medium Level of Confidence ○ Tortious Interference with Existing Contract ○ Tortious Interference with Prospective Contract, Business Relationship or Business Advantage ○ Fraudulent Misrepresentation ▪ High Level of Confidence ○ Defamation ○ Business or Commercial Disparagement
Create a statutory carve-out for existence of improper motive such that liability protection would no longer apply. To achieve this, there would need to be a standard set to trigger improper motive enough to limit the safe harbor.	▪ Tortious Interference with Existing Contract ▪ Tortious Interference with Prospective Contract, Business Relationship or Business Advantage ▪ Defamation ▪ Business or Commercial Disparagement
Consider a provision stating that SCRI demonstrating a high degree of risk (or that represents a violation of law) be legally mandated for disclosure to government. There would need to be a clarifying standard that would demonstrate a high degree of risk.	▪ Defamation ▪ Business or Commercial Disparagement ▪ Breach of Contract ▪ Misappropriation of Trade Secrets
Specific provision negating enforcement of contract terms for SCRI demonstrating a high degree of risk. Again, this requires a clarifying standard of what would demonstrate at high degree of risk.	▪ Breach of Contract ▪ Misappropriation of Trade Secrets

In addition to Table 2, WG1 offers the following additional general considerations, not directly tied to the causes of action in Table 1, to assist in framing potential legislation:

- Consider including a term providing for express preemption over conflicting federal or state laws
- Consider including a term providing an exemption for preservation of contracts, similar to that included in the CISA 2015, § 108(g), which states "Nothing in this title shall be

construed— (1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any entities, or between any entity and a Federal entity; or (2) to abrogate trade secret or intellectual property rights of any entity or Federal entity."

- Consider including an antitrust exemption to the extent SCRI-sharing poses concerns of federal antitrust violations. *See, e.g.,* CISA 2015, § 104(e)
- Consider a requirement that disclosing companies:
    - Submit only information that meets the definition for SCRI as agreed-upon by WG1 and shared in this report, and
    - Take reasonable steps to segregate and exclude extraneous information not directly bearing on the SCRI and omit this information from disclosure, including Personally Identifiable Information
- Consider including language that clarifies that data and information are covered items for the purposes of the definition of supply chain risk
- Consider recognizing the existing limits to the submission of personal information in CISA 2015

SUMMARY

In summary, WG1 offers the proposed updated definition and additional liability protections for consideration as ways to maximize protection for private entities seeking to take part in an SCRI-sharing framework and ultimately, improve the volume and quality of SCRI shared across and among the private and public sector. 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.

APPENDIX A

TABLE A-2—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
Tortious Interference with Prospective Contract, Business Relationship or Business Advantage	▪ Same considerations as Tortious Interference with Existing Contract apply ▪ Limitation of audience for disclosure	▪ Same provisions for Tortious Interference with Existing Contract apply ▪ Given consideration regarding audience for disclosure, risk is greater in making a private sector-to-private sector (or an ISAC) disclosure, than a disclosure to a secure governmental clearinghouse with restrictions on redistribution
Defamation	▪ Truth of statement ▪ Heightened degree of diligence undertaken and increased veracity of information ▪ Lack of improper purpose or malice (depending on the standard that applies) ▪ Limitations on dissemination	▪ Require Business A to possess a High[vii] level of confidence in the SCRI it shares ▪ 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 ▪ Consider provision stating that SCRI demonstrating a high degree of risk

CAUSE OF ACTION	MITIGATING FACTORS	PROPOSED CORRESPONDING SOLUTION OF SAFE HARBOR
	▪ Efforts taken to preserve identity of Business C ▪ Disclosure made in good faith or to further the public interest (some jurisdictions) ▪ Disclosure is required by law ▪ Disclosure is made to the government in a confidential fashion (some jurisdictions) ▪ Disclosure is made to law enforcement (some jurisdictions) ▪ Lack of proof of damages if not defamation per se	(or that represents a violation of law) be legally mandated for disclosure to government ▪ Limit disclosure to government for increased protection; separate carve-out for private parties or ISAC may be necessary
Business or Commercial Disparagement	▪ Most of the considerations applying to Defamation apply with equal weight ▪ Lack of intent to cause economic loss ▪ Lack of proof of damages	▪ Same provisions for Defamation would apply
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 at level of confidence in the SCRI it shares [viii]
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

CAUSE OF ACTION	MITIGATING FACTORS	PROPOSED CORRESPONDING SOLUTION OF SAFE HARBOR
	▪ Some protections exist for disclosure to government ▪ Encourage industry to include a contractual carve-out for disclosure of certain types of information or to allow for termination of contract should related-SCRI be discovered	public policy defense or government exception ▪ Additional protection providing immunity from breach of contract claims may be necessary
Misappropriation of Trade Secrets	▪ Similar considerations to Breach of Contract as breach can be prima facie evidence of misappropriation ▪ Having a right to the information ultimately disclosed may increase chances that a defense will apply	▪ Similar provisions to Breach of Contract as breach can be prima facie evidence of misappropriation ▪ Disclosure to government is safer than disclosure to private sector or ISAC

DHS POINT OF CONTACT

Cybersecurity and Infrastructure Security Agency
National Risk Management Center
U.S. Department of Homeland Security
NRMC@hq.dhs.gov
For more information about NRMC, visit www.cisa.gov/national-risk-management

---

[i] Pub. L. No. 114-113, 129 Stat. 2936, codified at 6 U.S.C. § 1501, et seq ("CISA 2015").

[ii] *See* CISA 2015 Sec. 106 (providing that "[n]o cause of action shall lie or be maintained in any court against any entity, and such action shall be promptly dismissed, for the sharing or receipt of cyber threat indicators or defensive measures under section 104(c) if (1) such sharing or receipt is conducted in accordance with this title; and (2) in a case in which a cyber threat indicator or defensive measure is shared with the Federal Government, the cyber threat indicator or defensive measure is shared in a manner that is consistent with section 105(c)(1)(B) …").

[iii] The following information sharing and reporting scenarios are separate and independent from considerations in this report:

(1) Breach Notification – should be distinguished from SCRI sharing as SCRI sharing is not contingent on an event occurring and involves information shared between sophisticated parties managing risk proactively rather than informing impacted individuals after the fact.

(2) Incident Reporting – may in some instances overlap with, follow, or precede SCRI sharing, but, as with breach notification, incident reporting is contingent on the occurrence of an event.

(3) Crime Reporting – like cyber incident reporting, crime reporting may overlap with, follow, or precede SCRI sharing, but does not directly correlate as terms and definitions in crime reporting scenarios generally relate to law enforcement investigations that can lead to criminal prosecution and thus carry different weight and meaning than their counterpart terms and definitions in operational SCRI sharing scenarios.

[iv] The Cybersecurity and Infrastructure Security Agency's ("CISA") Automated Indicator Sharing (AIS) Submission Guide, V. 16 (Jan. 2021) provides that a CISA analyst assign a Confidence rating to threat indicators and defensive measures based on the context of the event, validity of the source, and knowledge of the threat. See AIS Submission Guide, at PDF 15. These factors are used to develop specific confidence ratings, as follows:

- HIGH – This confidence is based on judgements of high-quality information from multiple sources or from a single, highly reliable source. This makes it possible to render a solid decision on the information.
- MEDIUM – The information is credibly sourced and plausible, but can be interpreted in various ways, or is not sufficient quality or collaborated sufficiently to warrant a higher level of confidence.
- LOW/UNKNOWN – The information's credibility and/or plausibility is questionable, the information is too fragmented or poorly collaborated to make solid analytical inferences, or that CISA has significant concerns or problems with the sources.

[v] Ibid, HIGH

[vi] Disclosure of SCRI to a government source or clearinghouse may provide greater liability protection than a private-to-private disclosure as narrow, secure disclosures may provide more insulation from liability than broader private-sector sharing efforts. A carve-out may exist for disclosure to a secure government clearinghouse to provide for mitigation of risk.

[vii] Ibid, HIGH

[viii] Ibid, confidence ratings