Health-ISAC®
SHARING SINCE 2010
Collaborating for Resilience in Health

CENTER FOR CYBERSECURITY POLICY AND LAW

WHITEPAPER

INFORMATION SHARING

U.S. Legal and Regulatory Guidance

FEBRUARY 2026

Abstract

Information sharing about cybersecurity threats and vulnerabilities produces enormous benefits — enabling entities to quickly learn about and protect against new and evolving attack vectors. Effective information sharing provides significant economic benefit for the organizations involved; helps protect companies against vulnerabilities being propagated by a weak link in the supply chain; and serves the broader public interest by improving security and resilience across the global community.

Within the United States, reaping the benefits of information-sharing programs can often be hindered by an incomplete understanding of legal risk. This document addresses those concerns. It assesses potential liability, available liability protections, and best practices for ensuring effective information sharing that mitigates legal risk.

Purpose of this document

Effective information sharing about new and evolving cyber threats can help organizations better manage those threats — with significant benefits to both the organizations involved and to the broader public. It is a collective action with collective benefits. It helps protect against an entity being the inadvertent vector for a threat that propagates through an entire sector – and beyond.

That said, private sector entities are often unsure about what can and should be shared, how to share information that does not inadvertently run afoul of legal and compliance obligations, and how to carry out information sharing in a way that minimizes liability risks.

This document addresses each of these considerations. It provides a reminder of the benefits of information sharing. It offers guidance on what can and should be shared, consistent with the overriding goal of creating a shared understanding and mitigating the risks of emergent threats; and it addresses the legal and compliance issues — suggesting best practices for sharing information while mitigating liability and other legal and reputational risks. That said, this document is not intended to constitute legal advice; entities should consult with counsel to help shape the specifics of any information-sharing agreement.

Why Share

Information sharing is foundational to good cybersecurity practice and the following outlines some of the many benefits of such sharing:

Improved Security Posture Through Shared Situational Awareness: Effective information sharing programs help participating organizations learn about – and thus mitigate the risk from – new and evolving threats. Doing so enables organizations to increase security, mitigate risk, and increase profitability. Absent such information sharing programs, organizations might not learn about new threats until malicious actors have already penetrated their systems.

Crowdsourced Cybersecurity Expertise: Participation in an information-sharing program allows organizations to tap into the pooled expertise and experiences of others. This collaboration enables organizations to leverage expertise within the community to improve their defenses, both generally and in response to specific attacks. These sharing communities also allow for organizations to learn from each other.

Heightened Community Trust and Resilience: A supply chain is only as strong as its weakest link. In today's connected and highly interdependent environments, a single weak link can wreak havoc on many other entities and the general public. By helping multiple and smaller entities to stay on top of continuously evolving cybersecurity threats, information sharing improves the security of the entire interconnected supply chain.

What to Share

Identification and sharing of threat intelligence is a central part of an effective information-sharing program. This includes information about malware, hacking techniques, and threat actors. But it is also much broader. Threat intelligence encompasses all risk vectors that could impact an organization or sector, such as third-party risks, insider threats, cybersecurity risks, regulatory risks, and geopolitical risks. These are the types of threats that organizations face daily and key elements of what should be included in an effective information-sharing program. The following describe key groupings of threat intelligence, broadly defined.

Strategic Intelligence

Strategic intelligence includes that which can help inform policy, set and/or justify information security budgets, and refine business plans at the corporate and divisional levels. Strategic intelligence typically focuses on new and emerging trends, evolutions in the cyber threat landscape, changes in laws and regulations, and the ever-evolving geopolitical and supply chain landscape.

Organizations can use strategic intelligence to proactively change their risk posture, meet regulatory compliance obligations, set a policy agenda, and preemptively mitigate emerging security threats. Strategic intelligence can help educate, prioritize, and cultivate proactive decision-making.

Tactical Intelligence

Tactical intelligence includes details about threat actor tactics, techniques, and procedures. As an example, tactical intelligence may detail exploitation methods that threat actors use to carry out credential harvesting attacks (e.g., credential dumping, brute force) or lateral movement (e.g., internal spear phishing, tainting shared content, and remote service exploitation). Tactical intelligence can help organizations prioritize defensive resources and provide clarity on threat vectors they should watch for.

Operational Intelligence

Operational intelligence is actionable information about specific weaponized attacks. Operational intelligence is typically gathered by monitoring the internet, social media platforms, and the dark web to provide early notification of vulnerabilities and potential or active attacks. Security researchers typically publish their research on new vulnerabilities and threats, and this is then shared amongst the community to provide members with awareness of active threats and mitigation strategies.

Who to Share With

The list of potential sharing partners is extensive and includes both internal and external considerations.

Internal Groups

Effective information sharing starts from within. The right internal stakeholders need to be engaged in the collection, analysis, and dissemination of information in order to ensure the implementation of appropriate mitigation measures and compliance with both internal policy and external legal and contractual obligations. Every organization will be different, but the following represents typical stakeholders to be included in internal information-sharing mechanisms:

- Cyber Threat Intelligence Teams
- Information Security Staff
- Legal Teams
- Senior Leadership
- Physical Security Staff
- Incident Response Teams
- Business Continuity and Disaster Recovery Professionals
- Education, Training & Awareness Teams

Policies and procedures should be in place to govern how internal sharing is conducted, and to ensure it is done in a systematic and documented manner.

External Partners

External information-sharing partners will vary based on the sector and regulatory frameworks in which organizations operate. However, it is common for organizations to consider information-sharing partnerships with critical suppliers and customers, law enforcement, and regulators. Additionally, organizations may wish to connect to the broader community of organizations within their given sector, through organizations like Information Sharing and Analysis Centers (ISACs).

In the case of Information Sharing and Analysis Centers (ISACs), for example, Membership Services Agreements (MSAs) typically outlines data sharing and classification requirements for the parties involved. MSAs are an essential tool for streamlining the sharing of information while putting appropriate protections and agreements into place. These organizational structures offer a medium for victims of a cyber intrusion to share their experiences safely and securely.

For example, pursuant to applicable MSAs, ISACs can share pertinent information in the wake of an attack, while keeping the victim's identity protected. ISACs can further vet the details of an incident, correct public misinformation, and provide clarity in a time of ambiguity.

Such agreements can be exclusively private-to-private or can include private-to-public sharing (and vice-versa). This can include sharing with regulators, non-regulatory government entities, and/or law enforcement.

Legal and Compliance Considerations

Private sector entities generally operate – rightly so – from the perspective that they need to protect proprietary information, intellectual property, and user privacy; avoid cooperation with competitors or others in ways that could invoke anti-trust concerns; and limit the sharing of information about specific operations and vulnerabilities. Information sharing agreements can, as a result, seem counter-intuitive to

lawyers and compliance officers who spend their days seeking to protect against the risks of liability and regulatory oversight.

Effective information-sharing agreements are designed in ways that mitigate the risks. This requires four key elements: clarity and limits about the kind of information that is shared; clarity and limits on how shared information is used; internal protocols for ensuring compliance with these limits; and engagement by counsel in all of the above.

The following addresses high-level legal and compliance considerations that are important elements of any effective information-sharing system. Specifically, it addresses the following: (i) anti-trust considerations; (ii) privacy laws; (iii) proprietary information and privilege issues; (iv) risk of regulatory actions; (v) FOIA considerations; and (vi) broader liability concerns. Importantly, each are directly addressed in the Cybersecurity Information Sharing Act of 2015 (CISA 2015), which provides key liability protections across each of these areas, with the goal of describing information sharing, as described below**.** As of this writing, the protections provided by CISA 2015, which temporarily expired in October of 2025 and briefly in February 2026, have been extended until the end of September 2026. The following offers general guidance as to how to think through each of these risks — both with and without the benefit of CISA 2015.

This is not meant to be legal advice but instead lays out key considerations for entities engaged in information-sharing agreements; entities should work with counsel to do individualized separate legal and compliance reviews, based on their specific situation.

Anti-Trust Considerations

Anti-trust liability can arise from the sharing of competitively sensitive information, when there is a finding of a "contract, combination, or conspiracy" that harms competition.

- *Liability Protections:* In response to concerns about potential anti-trust liability, Congress included broad anti-trust liability protection in CISA 2015. Specifically, the law provides exemptions from both federal and state antitrust laws for companies that share cyber-threat indicators or defensive measures for cybersecurity purposes. See 6 U.S.C. 1503(e). Consistent with the purposes of anti-trust law, these exemptions do not apply if the shared information is used for price-fixing, market allocation, or the exchange of competitively sensitive data.

- Even in the absence of CISA 2015, companies can avoid anti-trust liability by limiting information sharing cyber-threat indicators or defensive measures and avoiding the sharing of pricing information or other competitively sensitive information. In other words, CISA 2015 provides a useful prophylactic, helping to assuage concerns of those entities that might otherwise be concerned about anti-trust liability. But companies can engage in appropriately cabined cyber-threat information sharing, even without CISA 2015, without triggering anti-trust liability.

- Companies and/or information-sharing entities can also seek what is known as a "letter of exception" *from the Department of Justice and Federal Trade Commission. Such letters can explicitly protect entities from potential anti-trust liability in accordance with the stated terms.*

Privacy Considerations

Although there is no overarching federal privacy law in the United States, there are federal privacy requirements applicable to specific sectors (i.e., health, financial) that govern the sharing of certain personal information. Companies operating in the U.S. must also ensure their data sharing practices do not run afoul of federal and state prohibitions on unfair or deceptive acts or practices. Moreover, U.S. states and the European Union have passed comprehensive privacy laws that restrict the sharing of personal information (broadly defined to include data that can, alone or in combination with other information, identify an individual); federal and state regulators have taken legal action against entities for misrepresentations in their privacy policies; and privacy violations can cause significant reputational harm.

Notwithstanding these potential restrictions on personal information disclosures, entities can typically share data for threat reporting purposes without violating applicable privacy laws. As discussed above, entities should consult legal counsel, consider mitigations, and take steps in advance to ensure the desired sharing is supported by law. Relevant considerations include the following:

- *Mitigations:* Strategic threat reporting does not generally require the sharing of personal information that would trigger privacy law obligations or run afoul of privacy policies. Information-sharing agreements can and should be designed to minimize, if not fully eliminate, the sharing of personal information. If personal information must be shared, then companies may be able to structure privacy policies and agreements to make such sharing permissible under applicable law.

- *Liability Protection:* CISA 2015 explicitly requires organizations to remove or technically strip personal information not directly related to a cyber threat before sharing. See 6 USC § 1503(d)(2). CISA 2015 also provides broad liability protection for companies that share cyber threat indicators and defensive measures in good faith with the government or other private entities in accordance with this and other provisions of CISA 2015. See 6 USC § 1505(b).

- All U.S. state omnibus privacy laws effective through 2025, except the California Consumer Privacy Act (CCPA), contain broad security and fraud-related exemptions, clarifying that the laws do not restrict an organization's ability to reasonably prevent, detect, protect against, or respond to security incidents.

- Even though the CCPA exception is narrower than that included in other state laws, it still defines "[h]elping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate " as a legitimate "business purpose." See Cal. Civ. Code § 1978.140(e)(2). Sharing of personal information for a business purpose is permitted, but entities must enter an agreement with the recipient to ensure that the recipient complies with relevant privacy protections. In addition, entities are required to abide by certain notification and transparency requirements related to such sharing. Deidentified data is not subject to these restrictions.

- The EU's General Data Protection Regulation (GDPR) permits processing of personal data when it "is necessary for the purpose of the legitimate interests pursued by the controller or by a third party." Recitals 47, 49 and 50 of the GDPR collectively establish that the processing of personal data – to

include necessary and appropriate information sharing – for the purposes of preventing fraud, ensuring network security, or identifying possible criminal acts of threats to public security – is a legitimate interest. See also the Financial Services-ISAC analysis here.

Proprietary Information and Privilege Considerations

Overbroad information sharing can risk exposing intellectual property, trade secrets, or other proprietary information to competitors or adversaries, and could result in the waiver of otherwise applicable privileges (such as the attorney-client privileges).

- Appropriate cybersecurity information sharing should avoid these issues and ensure that participants do not disclose sensitive or proprietary business information or attorney-client protected information.
- *Explicit Statutory Protections for Information Shared with the Federal Government:* CISA 2015 expressly states that the sharing of such information with the federal government does waive any applicable privilege, including trade-secret protection. See 6 U.S.C. § 1504(d)(1). The law provides an explicit mechanism by which organizations can designate information shared with the federal government as commercial, financial, and proprietary, and thus treated accordingly. See 6 U.S.C. § 1504(d)(2).
- The CISA 2015 provisions only apply to sharing with the federal government. As an added protection for private-to-private information sharing, information sharing bodies can and should protect against dissemination of other entities' information. The Health-ISAC Code of Conduct, for example, explicitly prohibits members from using, disclosing, or releasing another member's intellectual property

Risk of Regulatory Scrutiny or Enforcement

A range of federal and state regulations require breach reporting; failure to do so can result in fines. Regulators also seek to enforce against deceptive trade practices, in which entities do not abide by material representations made to their customers.

- *Explicit Protections:* To encourage the sharing of cyber threat indicators, CISA 2015 bars any federal, state, tribal, or local government from using shared information to regulate or enforce against the entity for related activities. *See* 6 U.S.C. §1504(d)(5)(D). Regulators can, however, use that information to inform the development or implementation of regulations related to prevention or mitigation of cyber threats to information systems; regulators just can't use the information to enforce against the entity that shared.

Freedom of Information Act (FOIA) Requests

When information is shared with the government, there is the possibility that it eventually becomes the subject of a FOIA request. There are multiple exceptions to the disclosure obligations under FOIA, to include exceptions for commercial and financial information and trade secrets, matters compiled for law enforcement purposes, and matters subject to an explicit statutory exception.

- *Explicit Statutory Exceptions:*
    - CISA 2015 provides one of the applicable and explicit statutory exceptions to disclosure requirements under FOIA. It categorically exempts information shared in accordance with the Act from FOIA and similar state or local disclosure laws. *See* 6 U.S.C. §1504(d)(3)).
    - Pursuant to the Critical Infrastructure Information Act of 2002, critical infrastructure information voluntarily shared with the Department of Homeland Security for use in ensuring the security of critical infrastructure is also categorically protected from FOIA and state disclosure laws. *See* 6 U.S.C. § 673(a).
- In the absence of these statutory exceptions, entities should, in coordination with counsel, set up protocols to ensure information shared with the federal government is covered by an applicable FOIA exception and/or possible release of the information does not pose concerns.

Broader Liability Concerns

Some worry about the possibility that information shared about a cyber event, incident, or vulnerability could lead to or be included as relevant evidence in lawsuits from customers, shareholders, or other affected parties.

- *Explicit Protections:*
    - CISA 2015 provides broad liability protection "in any [U.S.] court" for claims based on the sharing or receiving cyber-threat indicators or defensive measures, provided the sharing is done in good faith with the government or other private entities. *See* 6 U.S.C. §1505(d).
    - The Critical Infrastructure Act of 2002 provides broad protection against use of critical infrastructure information voluntarily shared with the Department of Homeland Security in good faith in "any civil action," absent explicit consent by the party that shared the relevant information. *See* 6 U.S.C. § 673(a)(1)(C).

Conclusion

Responsible information sharing agreements can provide significant ecosystem-wide security benefits. In recognition of these benefits, Congress has created legally protected avenues to share pertinent information. But even without (or as a supplement to) these statutory protections, private agreements that clearly define and place responsible limits on what information is shared and how it is disseminated can also mitigate any potential legal risk.

We encourage organizations that have been reticent to share information to reconsider that approach. We also encourage those already engaged in information sharing activities (such as ISACs or Sector Risk Management Agencies (SRMAs)) to use this guidance to re-examine the scope of existing information sharing and the protections in place – and ensure that both are maximized to their fullest potential. To reiterate, this Guidance is not legal advice. Each entity and organization should engage with legal counsel to

do individualized assessments of the key considerations and potential risks. That said, this Guidance can provide a useful frame for such discussions.

About the Authoring Organizations

The **Center for Cybersecurity Policy and Law** is a nonprofit 501(c)(6) organization that develops, advances, and promotes best practices and educational opportunities among cybersecurity professionals. The Center provides a forum for thought leadership for the benefit of those in the industry, including members of civil society and government entities in the area of cybersecurity and related technology policy. The Center seeks to leverage the experience of leaders in the field to ensure a robust marketplace for cybersecurity technologies that will encourage professionals, companies, and groups of all sizes to take steps to improve their cybersecurity practices.

To learn more about the Center and our wide-ranging initiatives, please visit https://centerforcybersecuritypolicy.org.

The **Health-ISAC** (Health Information Sharing and Analysis Center) is a non-profit, member-driven organization dedicated to protecting the global health sector from cyber and physical threats. Through real-time alerts, collaboration, and usable intelligence, Health-ISAC helps healthcare organizations improve security and resilience.

To learn more about the Health-ISAC, please visit
www.health-isac.org