Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

April 8, 2025

The Cybersecurity Information Sharing Act of 2015: Expiring Provisions

A decade ago, Congress authorized a cybersecurity information sharing structure that allows the federal government to collect and disseminate threat information, and enabled private sector entities to voluntarily share that information with the government, as well as among themselves. Congress passed this authorization after discussing the need for an information sharing protection framework with stakeholders in order to amplify their collective understanding of cybersecurity threats and how to respond to them. The provisions in this authorization are set to expire on September 30, 2025. A number of industry groups have advocated for its renewal.

This CRS In Focus discusses these provisions, potential implications for their expiration, and possible changes to statute that Congress may choose to consider.

Background

Congress passed the Cybersecurity Information Sharing Act of 2015 (act) as Title I of the Cybersecurity Act of 2015. The major authorizing provisions prescribe that

- Agencies with cyber threat information shall have procedures to share that information in a classified and unclassified way with both federal and nonfederal entities.
- An entity (governmental or nongovernmental) can have a private sector entity monitor and secure their information technology (IT).
- Private entities may share information related to identifying and defending against cyberthreats with other private entities and with the federal government.
- The private sector will not be subject to antitrust liability for participating in the cybersecurity information sharing activities authorized by the act.
- Personally identifiable information (PII) must be removed from shared information. Further, the Department of Homeland Security (DHS) and Department of Justice (DOJ) shall release guidance on protecting civil liberties when sharing information.
- The DHS and DOJ shall issue guidance on federal government and nonfederal entity information sharing.
- Private entities shall be protected from liability when conducting certain act-authorized activities, including monitoring IT, implementing protective actions, and sharing cybersecurity information.
- Information shared under the act is exempt from federal and state disclosure requirements.

The Senate Select Committee on Intelligence committee report on the originally-considered bill highlights some of the areas of debate. In 2015, privacy protections for the information of individuals that could potentially be collected and shared through the program, and limitations on the use of program information were of primary concern. Recent Inspector General reviews have not found that PII has been shared in violation of the act.

Automated Indicator Sharing Program

The Automated Indicator Sharing Program (AIS) implements the information sharing requirements prescribed by the act. It is voluntary program which allows the federal government and nonfederal participants to share certain *indicators* of cybersecurity threat information with each other.

The program defines an indicator as a "technical artifact or observable that suggests an attack is imminent or is currently underway, or that a compromise may have already occurred." Examples of such indicators might include a malicious website, activity by a known threat actor, or the identification of a new technique.

The AIS primarily shares indicators provided by government agencies. These indicators could be gained from both an unclassified source (e.g., reported by a regulated entity) or a classified source (e.g., collected through a classified program or operation, even if the information itself is unclassified). These indicators are uploaded into an AIS server which pushes that information to program participants. AIS also collects indicators from the private sector, which are voluntarily shared.

To participate in the program, an entity (federal or nonfederal) agrees to participation in writing and establishes an AIS client server. The entity then connects the AIS client server to their IT and cybersecurity equipment to enable real-time, machine-to-machine information sharing. AIS is a technical capability, but the information could potentially be shared in other ways (e.g., manual reporting) and still receive protections under the act

because an agreement is in place. For example, a group of companies may use the technology developed for AIS to share information amongst themselves, but rely on their sector's information sharing and analysis organization (ISAO) to submit that information to the government.

Implications of Expiration

If Congress allows the act to expire, then changes in cybersecurity information sharing practices may affect both the government and private sector.

The information protection measures, antitrust protections, liability protections, and protections from disclosure (e.g., in court proceedings) that are explicit and specific to the act would be affected by the act's expiration. Without these protections, private sector entities may be less willing to share cyber threat information with the federal government and each other. Lacking that private sector information, the federal government may find itself in the same position that drove passage of the act—not knowing the extent of current cyber threats and lacking the information necessary to mitigate those threats.

Further, the ability for the private sector to exchange information and provide technical assistance on threats, and the marketplace for the provision of cybersecurity services to other companies, may collapse without these explicit authorizations.

The absence of the act's authorizations may not affect the technical capabilities DHS created to enable the AIS program, as DHS was working on creating that program under other information sharing authorities prior to the act.

Considerations for Reauthorization

Congress may choose to do a *clean extension*, whereby only the expiration of the act is amended to a later date. Congress may also choose to alter other aspects of the act in legislation that amends the expiration date. Congress may also choose alternative legislative vehicles entirely in lieu of or in addition to extension of the act.

Duration of a Potential Extension

Congress originally authorized the act for 10 years. Congress may choose to extend this period for any duration lawmakers wish. This may be for a matter of months as an interim measure, a finite period (potentially years), or an indefinite continuance. A shorter-term extension may provide Congress additional time to observe how the authorities in the act interact with newer cybersecurity provisions (e.g., cyber incident reporting or minimum standards). A longer-term authorization may provide stakeholders (including the private sector) with more certainty concerning their ability to implement and benefit from the act's provisions, procedures for information sharing, and liability protections when taking action against cybersecurity threats.

Changing Definitions

During the decade since enactment, risks to cyberspace have evolved. One risk which has risen in prominence is the targeting of nontraditional IT, including *operational technology* (OT) and *edge devices*. Operational technology connects IT with physical systems. Examples include *industrial control systems* (such as those which monitor gas pipelines for line pack and pressure) and its components, including *supervisory control and data acquisition* (SCADA) systems (such as those that facilitate safety operations at dams and powerplants). Edge devices are a type of *information and communications technology* used to connect one network to another (e.g., a home router). Nation-state actors and cyber criminals have targeted OT and edge devices; however, these technologies are not explicitly captured by the definitions currently contained within the act. Furthermore, artificial intelligence is not specifically addressed in the act. Some observers think it vital for Congress to include expanded definitions in a reauthorization in order to provide stakeholders clarity on which types of threat information are encouraged to be shared and are protected under the act. Congress may choose to consider expanding the act's definitions to include novel attack vectors and/or new methods of defense, or generalizing the language to allow for future technological developments.

Information Sharing Mandates

Congress may also choose to consider whether program participation should remain voluntary. The Senate committee report made clear that, at the time the act was debated, the committee was seeking to create a voluntary information sharing program. Since the act, Congress created a mandatory cyber incident reporting framework through the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). CIRCIA requires that certain entities report to the government when they experience a cybersecurity incident or make a ransomware payment. CIRCIA's passage reflected a substantive change in the nature of cybersecurity data collection, whereby the government deemed it necessary to require the private sector to submit information to a federal agency in order for the government to have a more complete picture of cyberattacks across the nation.

While both the act and CIRCIA provide cybersecurity information to the government, they do so in tandem and not as a replacement for each other. The former provides potentially incident-preventing information. The latter seeks to understand elapsed events in order to prevent future ones. Further, the act provides a structure for continual, omnidirectional information sharing, where CIRCIA provides for occasional, unidirectional reporting by industry or government.

Congress may choose to consider whether or not to require certain entities to share cyber threat information under the Cybersecurity Information Sharing Act. For example, Congress could require aggregators of cyber threat information (e.g., cybersecurity firms or cloud service providers) or critical infrastructure entities (e.g., healthcare or financial institutions), a subset of those categories, or a broader group of participants to share cyber threat information under the act.

Chris Jaikaran, Specialist in Cybersecurity Policy

IF12959

Disclaimer