GAO
U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Snapshot

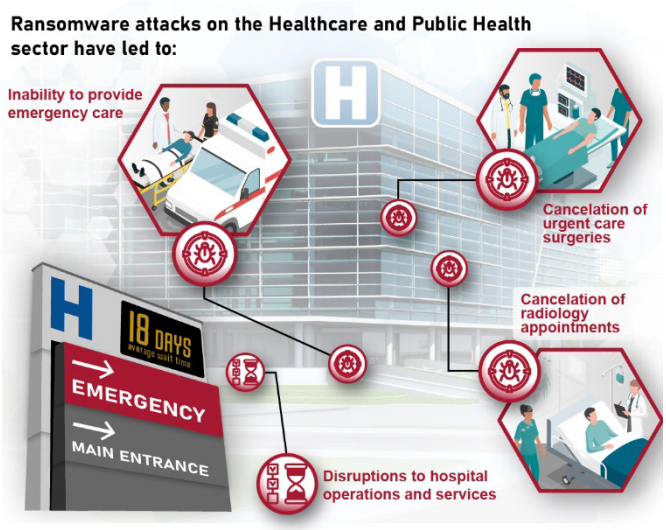
Cybersecurity: Implementation of the 2015 Information Sharing Act

GAO-25-108509, July 2025

Policies and actions implemented under the Cybersecurity Information Sharing Act of 2015 have positively contributed to the sharing of cyber threat information between federal and nonfederal entities. Sharing such information can enhance awareness of the extent of current cyber threats and how to mitigate those threats.

The Big Picture

Malicious cyberattacks on the federal government and the nation's critical infrastructures, such as electricity and healthcare, are growing in number, impact, and sophistication and have led to significant disruptions.



Sources: GAO analysis of publicly reported incident information; GAO (sign); elenabsl/stock.adobe.com (images); archipoch/stock.adobe.com (hospital); motorama/stock.adobe.com (icons). | GAO-25-108509

The Cybersecurity Information Sharing Act of 2015, which sunsets on September 30, 2025, encourages the sharing of (1) **cyber threat indicators** that provide information on malicious attempts to compromise a system and (2) **defensive measures** taken against cyber threats. Sharing such information can enhance federal and nonfederal awareness of the extent and type of current cyber threats and attacks, and mitigation techniques to minimize their impact. The act also requires agencies to protect privacy and civil liberties by removing personally identifiable information from shared cyber threat indicators.

In this Snapshot, we highlight the actions of seven agencies designated to implement the act—the Departments of Homeland Security, Justice, Defense, Commerce, Energy, and the Treasury; and the Office of the Director of National Intelligence.

What GAO's Work Shows

We have reported on broad cyber threat information sharing activities, including efforts to implement the act. The Office of the Inspector General of the Intelligence Community (ICIG) has also compiled reports from each agency's inspector general showing the extent to which agencies have implemented the act.

Agencies Met the Act's Requirements for Sharing Threat Information and Removing Personally Identifiable Information

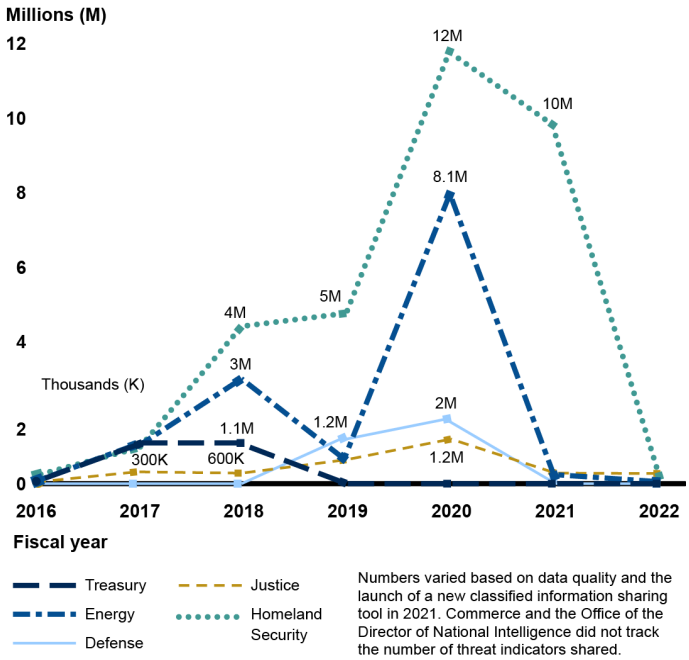
In 2023, we reported that all seven federal agencies developed government-wide policies, procedures, and guidelines to help federal and nonfederal entities receive and share cybersecurity information, as required by the act. We also reported in 2018 that all seven agencies developed final guidelines related to privacy and civil liberties that govern how threat information is received, used, retained, and distributed to protect personally identifiable information.

The ICIG reported in 2023 that federal agencies met the provisions of the act. For example, agencies: (1) properly classified all shared information; (2) disseminated, shared, and received threat information and defensive measures in a timely and adequate manner; (3) removed personally identifiable information prior to sharing information; and (4) identified barriers that have hindered sharing such information.

The Act Enabled the Development of Data Sharing Tools

Prior to the act, nonfederal entities did not have a readily available method of sharing cyber threat information. However, the act led to the development of automated information sharing tools for entities to share classified and unclassified threat information. As of 2023, agencies continue to use those tools and other reporting means such as email, written reports, websites, and face-to-face communication. The ICIG's biennial reports from 2017, 2019, 2021, and 2023 described the estimated number of threat indicators and defensive measures shared over the years by five agencies using the unclassified automated information sharing tool.

Estimated Number of Threat Indicators and Defensive Measures Shared Using the Unclassified Automated Sharing Tool



Source: GAO analysis of Intelligence Community Inspector General reports. | GAO-25-108509

Reported Barriers and Opportunities

The act also requires that agencies report barriers to sharing cyber threat information. The ICIG has reported several long-standing barriers to sharing threat information and defensive measures.

Agency-Reported Barriers to Sharing Cyber Threat Information, Calendar Years 2016-2022

Reluctance to share information	• Some nonfederal entities are hesitant to share cyber threat information because it might raise legal issues or lead to negative business penalties.
Classification concerns	• Agencies cannot transfer classified threat information to an unclassified environment. Some agencies do not have staff with the appropriate security clearance to receive classified threat information.
Challenges with the unclassified information sharing tool	• Data does not always contain the necessary context or contains duplicated indicators. • The tool is not easily searchable and requires staff to manually sort through information.
No policy requirement	• Agencies tend not to share because there is no requirement to do so.
Inconsistent format	• Federal threat indicator repositories do not enable flexible sharing of threat information because some file formats are not compatible with the data format in the receiving entity's repository.
Resource constraints	• There are no automation tools to process threat information and remove personally identifiable information. As a result, agencies require more technically trained individuals to review data. • Mis-categorization of threat information can make it difficult to effectively filter and sort relevant information.

Source: GAO analysis of Intelligence Community Inspector General reports. | GAO-25-108509

In 2023 we reported on federal actions planned and underway to address some of these barriers.

- The Cybersecurity and Infrastructure Security Agency (CISA) and other related entities planned to make declassifying and disseminating unclassified elements of threat indicators contained within classified systems easier.
- CISA enhanced the unclassified information sharing tool platform to address challenges with data quality and timeliness. CISA planned to update guidance for connecting to the tool and streamline the onboarding process.
- CISA had agreements with 15 third-party threat intelligence companies to make the tool more accessible for agencies with technical challenges and minimize agency costs.

Contact Us:

For more information, contact: David B. Hinchman, HinchmanD@gao.gov.

Public Affairs: Sarah Kaczmarek, Managing Director, Media@gao.gov.

Congressional Relations: A. Nicole Clowers, Managing Director, CongRel@gao.gov.

Contributors: Kavita Daitnarayan, Michael Gilmore, Smith Julmisse, Jess Lionne, Scott Pettis, and Dwayne Staten.

Source (cover photo): adam121/stock.adobe.com