GAO Highlights

Highlights of GAO-23-105468, a report to congressional addressees

September 2023

CRITICAL INFRASTRUCTURE PROTECTION

National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods

Why GAO Did This Study

Cyber threats to the nation's critical infrastructure sectors are significant. As such, it is important that federal agencies and critical infrastructure owners and operators share cyber threat information. ONCD and CISA lead federal efforts to coordinate on national cyber policy and the security of critical infrastructure.

This report examines, among other things, (1) how federal agencies and critical infrastructure owners and operators share cyber threat information and (2) challenges to cyber threat information sharing and the extent to which federal agencies have taken action to address them.

To do so, GAO reviewed documentation from 14 federal agencies, including CISA, and seven nonfederal entities with responsibility for sharing cyber threat information. In addition, GAO interviewed relevant officials from these federal agencies and nonfederal entities regarding challenges to sharing cyber threat information.

Using information compiled from interviews, GAO then presented the cyber threat information challenges frequently identified by the relevant entities to the 14 federal agencies and ONCD. GAO also asked for and reviewed documentation on actions the 14 agencies and ONCD have taken or plan to take to address the challenges.

In addition, GAO compared the *National Cybersecurity Strategy* and accompanying implementation plan with its prior work on leading practices for national strategies and business process reengineering.

View GAO-23-105468. For more information, contact Marisol Cruz Cain at (202) 512-5017 or CruzCainM@gao.gov or Tina Won Sherman at (202) 512-8461 or ShermanT@gao.gov.

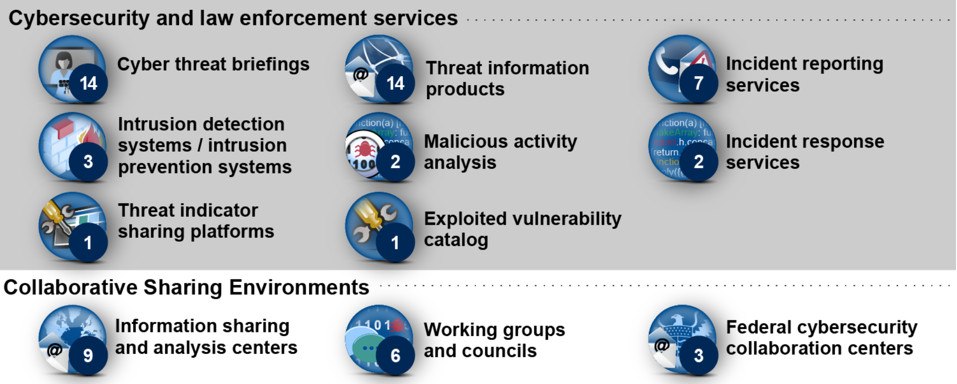
What GAO Found

The nation's 16 critical infrastructure sectors rely on electronic systems to provide essential services such as electricity, communications, and financial services. Federal entities have key roles in helping to protect these sectors.

- The Office of the National Cyber Director (ONCD) is to advise the President on cybersecurity policy and strategy, and lead the coordination of implementation of the March 2023 *National Cybersecurity Strategy*.
- The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is to coordinate the overall federal effort to promote the security of the nation's critical infrastructure, including the sharing of threat information.
- The FBI is to lead counterterrorism and counterintelligence investigations and related law enforcement activities across the critical infrastructure sectors and share related cyber threat information.
- CISA and 12 other agencies are sector risk management agencies responsible for providing specialized expertise for protecting the cybersecurity of their assigned sectors (e.g., Department of Energy and the energy sector), to include the sharing of sector-specific threat information.

The 14 federal agencies in GAO's review—CISA, FBI, and the other 12 sector risk management agencies—reported relying on 11 methods to facilitate sharing of cyber threat information with critical infrastructure owners and operators. As shown in figure 1, these agencies used each of the 11 methods to varying degrees (see the numbers next to each method).

Figure 1: Number of Methods Used by 14 Federal Agencies Sharing Cyber Threat Information


Cybersecurity and law enforcement services
14 Cyber threat briefings
14 Threat information products
7 Incident reporting services
3 Intrusion detection systems / intrusion prevention systems
2 Malicious activity analysis
2 Incident response services
1 Threat indicator sharing platforms
1 Exploited vulnerability catalog
Collaborative Sharing Environments
9 Information sharing and analysis centers
6 Working groups and councils
3 Federal cybersecurity collaboration centers

Sources: GAO analysis of cyber threat sharing methods, and images/icons. | GAO-23-105468

The 14 agencies varied in the number of information sharing methods that they each used. Specifically, four agencies—the Department of Defense, the Department of Energy, CISA, and FBI—used more than half of the 11 sharing methods and 10 agencies used fewer than half of the 11 sharing methods.

The agencies took two different approaches to using the 11 sharing methods. Specifically, two agencies—CISA and FBI—used a centralized approach to share information with each of the 16 critical infrastructure sectors. The other 12 remaining federal agencies shared sector-specific threat information.

What GAO Recommends

GAO is recommending that:

(1) ONCD identify outcome-oriented performance measures for the cyber threat information sharing initiatives included in the *National Cybersecurity Strategy* implementation plan, and

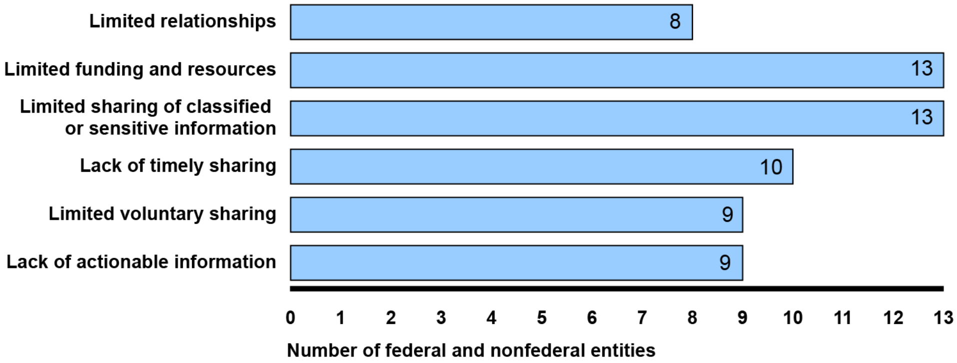
(2) CISA assess whether the current mix of centralized and sector-specific sharing methods used by agencies is the optimal approach to addressing cyber threat sharing challenges.

In commenting on a draft of this report, ONCD agreed with GAO's finding on outcome-oriented measures but disagreed with the recommendation. As discussed in the report, GAO continues to believe that this recommendation is necessary to evaluate the effectiveness of planned efforts. Based on additional contextual information provided by ONCD, GAO withdrew from its report one recommendation on voluntary and timely information sharing.

DHS concurred with the recommendation to CISA.

Six challenges to effective sharing of cyber threat information were identified by at least a third of the 21 entities in GAO's review (14 federal agencies and seven nonfederal entities) (see figure 2).

Figure 2: Six Challenges to Cyber Threat Information Sharing Identified by Federal Agencies and Nonfederal Entities



Source: GAO analysis of factors that challenged cyber threat information sharing. | GAO-23-105468

Although 13 of the 14 federal agencies reported that they have taken initial actions to address these threat sharing challenges, all 14 agencies also acknowledged that these challenges have not been fully resolved for their sectors. In March and July 2023, the White House issued its *National Cybersecurity Strategy* and accompanying implementation plan to articulate the administration's plan for addressing the nation's long-standing cybersecurity challenges—including those pertaining to information sharing. The implementation plan includes eight initiatives that, if effectively implemented, could help agencies make progress in addressing the cyber threat information sharing challenges. For example, the implementation plan includes an initiative focused on removing barriers to delivering cyber threat intelligence. This initiative could help agencies make progress in addressing the challenge of limited sharing of classified or sensitive information.

GAO's prior work emphasizes the importance of (1) identifying outcome-oriented performance measures and (2) assessing whether existing processes are optimal for addressing challenges.

- The implementation plan does not identify outcome-oriented performance measures to assess the effectiveness of the steps taken under the eight information sharing initiatives described in the plan.
- The long-standing nature of the cyber threat sharing challenges raises questions about whether the mix of centralized and sector-specific sharing approaches is optimal. Although the implementation plan calls for CISA to assess whether new or improved sharing methods are needed, it does not include an assessment of whether existing sharing methods should be retired in favor of centralized or sector-specific sharing approaches.

Until the ONCD and CISA take steps to resolve these weaknesses, the long-standing cyber threat sharing challenges will likely continue to persist.