GAO Highlights

Highlights of GAO-24-106576, a report to congressional committees

March 2024

CYBERSECURITY

Improvements Needed in Addressing Risks to Operational Technology

Why GAO Did This Study

Much of the nation's critical infrastructure relies on OT—systems that interact with the physical environment—to provide essential services. However, malicious cyber actors pose a significant threat to these systems. Federal law designates CISA as the lead agency in helping critical infrastructure owners and operators address cyber risks to OT.

The National Defense Authorization Act of Fiscal Year 2022 includes a provision for GAO to report on CISA's support for industrial control systems. Federal guidance now addresses these systems under the broader category of OT. Accordingly, this report examines, among other things: (1) challenges in delivering CISA's OT products and services, and (2) challenges to collaborating between CISA and the seven selected agencies.

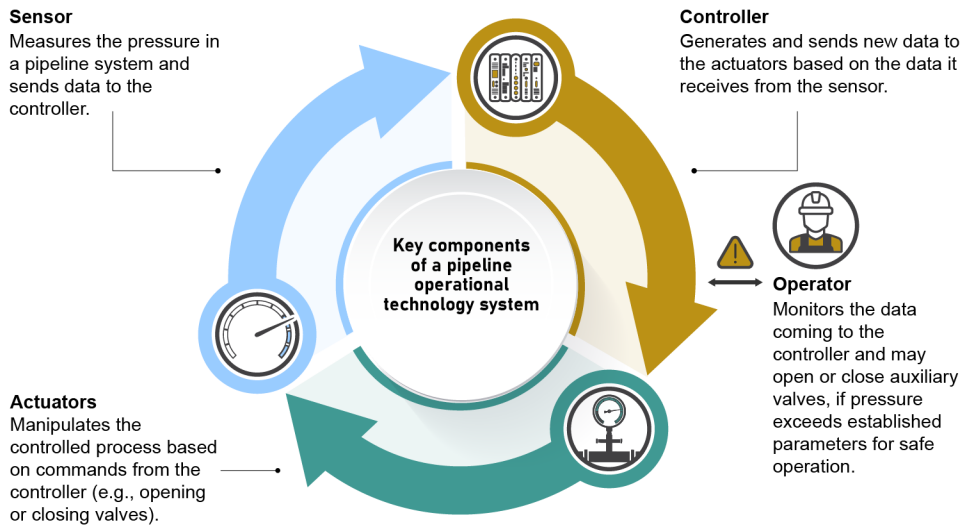
GAO reviewed documentation describing CISA's 13 OT cybersecurity products and services. GAO also asked officials from CISA and 13 selected nonfederal entities to identify any challenges with the OT products and services. The selected entities included (1) councils representing one sector and three subsectors where OT was prevalent and the intelligence community highlighted their infrastructures as being at risk from cyber threat actors, (2) OT vendors who joined a CISA OT collaboration group, and (3) cybersecurity researchers that contributed to the development of CISA's OT advisories. GAO then compared CISA's efforts to address those challenges against leading practices regarding measuring customer service and workforce planning.

View GAO-24-106576. For more information, contact Marisol Cruz Cain (202) 512-5017 or CruzCainM@gao.gov.

What GAO Found

Operational technology (OT) systems and devices are used to control, among other things, distribution processes (e.g., oil and natural gas pipelines) and production systems (e.g., electric power generation). Figure 1 shows the key components of an OT system using a pipeline system as an illustrative example.

Figure 1: Key Components of a Pipeline Operational Technology (OT) System



Sources: GAO (analysis and icons); staratel/stock.adobe.com (icons); iconlauk/stock.adobe.com (icon). | GAO-24-106576

Although 12 of the 13 selected nonfederal entities cited examples of positive experiences with the Cybersecurity and Infrastructure Security Agency's (CISA) OT products and services, CISA and seven of the nonfederal entities identified two types of associated challenges. Specifically:

- Seven selected nonfederal entities identified **negative experiences using CISA's products and services** as a challenge. For example, one nonfederal entity told GAO that vulnerabilities reported through CISA's process often take more than a year between the initial report of a vulnerability and public disclosure (see figure 2).
- CISA officials and one nonfederal entity identified the **insufficient CISA staff with requisite OT skills** as a challenge. For example, CISA officials stated that its four federal employees and five contractor staff on the threat hunting and incident response service are not enough staff to respond to significant attacks impacting OT systems in multiple locations at the same time.

To address these types of challenges, best practices highlight the importance of (1) measuring customer service and (2) performing effective workforce planning. However, CISA has not fully addressed these practices. Until CISA does so, the agency will not be optimally positioned to deliver products and services needed to address OT risks.

In addition, GAO reviewed documentation describing CISA's efforts to collaborate with seven selected agencies to mitigate cyber OT risks. The seven selected agencies are: (1) Department of Defense's (DOD) Defense Cyber Crime Center (DC3); (2) DOD's National Security Agency (NSA); (3) Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER); (4) Department of Homeland Security's (DHS) Transportation Security Administration (TSA); (5) DHS's U.S. Coast Guard (USCG); (6) Department of Transportation's (DOT) Federal Railroad Administration (FRA); and (7) DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA). GAO focused on these agencies or departmental components because each was (1) within agencies designated as the lead for helping to protect the selected sector and three subsectors and (2) responsible for helping critical infrastructure owners and operators to mitigate cyber OT risks. GAO also asked officials from seven selected agencies to identify any challenges in collaborating with CISA to mitigate cyber OT risks. GAO then compared documentation from the seven agencies and CISA against five selected leading collaboration practices.

What GAO Recommends

GAO is making four recommendations to CISA to implement processes and guidance to improve its OT products and services and collaboration. Specifically, GAO is recommending that CISA

1. measure customer service for its OT products and services,
2. perform effective workforce planning for OT staff,
3. issue guidance to the sector risk management agencies on how to update their plans for coordinating on critical infrastructure issues, and
4. develop a policy on agreements with sector risk management agencies with respect to collaboration.

DHS concurred with the four recommendations to CISA and described actions that the agency plans to take to implement them.

Figure 2: Cybersecurity and Infrastructure Security Agency (CISA) Operational Technology (OT) Cybersecurity Products and Services

Source: CISA (documentation and icons). | GAO-24-106576

Six of the seven selected agencies cited examples of where their collaboration with CISA yielded positive outcomes to addressing cyber OT risks. However, four agencies also identified two challenges in coordinating with CISA: (1) CISA ineffectively sharing information with critical infrastructure owners and operators, and (2) CISA and the Pipeline and Hazardous Materials Safety Administration lacking a process to share cyber threat information with owners and operators.

To address these types of challenges, it is important to adopt leading collaboration practices. However, CISA did not fully address any of five selected leading collaboration practices when coordinating with seven selected agencies (see table).

Extent to Which the Cybersecurity and Infrastructure Security Agency (CISA) Addressed Selected Leading Collaboration Practices with Seven Selected Agencies to Mitigate Cyber Operational Technology Risks to Critical Infrastructure

Collaboration practices	CESER	DC3	FRA	NSA	PHMSA	TSA	USCG
Define common outcomes	◑	◑	◑	◑	◑	◑	◑
Ensure accountability	○	○	◑	○	◑	◑	◑
Bridge organizational cultures	◑	◑	◑	◑	◑	◑	◑
Clarify roles and responsibilities	◑	◑	◑	◑	◑	◑	◑
Develop and update written guidance and agreements	○	◑	○	○	○	○	◑

Source: GAO analysis of agency information. | GAO-24-106576

Legend: ●=Generally addressed. ◑=Partially addressed. ○=Not addressed.

Note: CESER (Cybersecurity, Energy Security, and Emergency Response), DC3 (Department of Defense Cyber Crime Center), FRA (Federal Railroad Administration), NSA (National Security Agency), PHMSA (Pipeline and Hazardous Materials Safety Administration), TSA (Transportation Security Administration), and USCG (U.S. Coast Guard).

The practices were not fully addressed, in part, because of the lack of (1) guidance from CISA to the sector risk management agencies on how to update their plans for coordinating on critical infrastructure issues and (2) a CISA policy for developing agreements with sector risk management agencies with respect to collaboration. Until CISA takes action to address these weaknesses, it and the selected agencies will not be well-positioned to coordinate on mitigating cyber OT risks.