Highlights of GAO-25-107435, a report to congressional addressees

Why GAO Did This Study

Al has the potential to introduce improvements and rapidly change many areas. However, deploying Al may make critical infrastructure systems that support the nation's essential functions, such as supplying water, generating electricity, and producing food, more vulnerable. In October 2023, the President issued Executive Order 14110 for the responsible development and use of Al. The order requires lead federal agencies to evaluate and, beginning in 2024, annually report to DHS on Al risks to critical infrastructure sectors.

GAO's report examines the extent to which lead agencies have evaluated potential risks related to the use of AI in critical infrastructure sectors and developed mitigation strategies to address the identified risks. To do so, GAO analyzed federal policies and guidance to identify activities and key factors for developing AI risk assessments. GAO analyzed lead agencies' 16 sector and one subsector risk assessments against these activities and key factors. GAO also interviewed officials to obtain information about the risk assessment process and plans for future templates and guidance.

What GAO Recommends

GAO is recommending that DHS act quickly to update its guidance and template for AI risk assessments to address the remaining gaps identified in this report. DHS agreed with our recommendation and stated it plans to provide agencies with additional guidance that addresses gaps in the report including identifying potential risks and evaluating the level of risk.

View GAO-25-107435. For more information, contact David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov; or Tina Won Sherman at (202) 512-8461 or shermant@gao.gov.

December 2024

ARTIFICIAL INTELLIGENCE

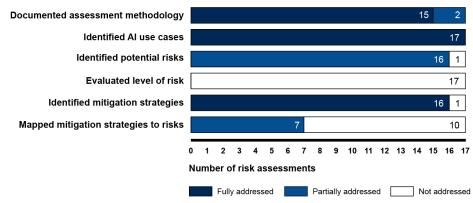
DHS Needs to Improve Risk Assessment Guidance for Critical Infrastructure Sectors

What GAO Found

Federal agencies with a lead role in protecting the nation's critical infrastructure sectors are referred to as sector risk management agencies. These agencies, in coordination with the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), were required to develop and submit initial risk assessments for each of the critical infrastructure sectors to DHS by January 2024. Although the agencies submitted the sector risk assessments to DHS as required, none fully addressed the six activities that establish a foundation for effective risk assessment and mitigation of potential artificial intelligence (AI) risks. For example, while all assessments identified AI use cases, such as monitoring and enhancing digital and physical surveillance, most did not fully identify potential risks, including the likelihood of a risk occurring. None of the assessments fully evaluated the level of risk in that they did not include a measurement that reflected both the magnitude of harm (level of impact) and the probability of an event occurring (likelihood of occurrence). Further, no agencies fully mapped mitigation strategies to risks because the level of risk was not evaluated.

Extent to Which the Sector Risk Management Agencies (SRMA) Have Addressed Six Activities in Their Sector Risk Assessments of Artificial Intelligence (AI)

Activities



Source: GAO analysis of critical infrastructure sector AI risk assessments. | GAO-25-107435

Lead agencies provided several reasons for their mixed progress, including being provided only 90 days to complete their initial assessments. A key contributing factor was that DHS's initial guidance to agencies on preparing the risk assessments did not fully address all the above activities.

DHS and CISA have made various improvements, including issuing new guidance and a revised risk assessment template in August 2024. The template addresses some—but not all—of the gaps that GAO found. Specifically, the new template does not fully address the activities for identifying potential risks including the likelihood of a risk occurring. CISA officials stated that the agency plans to further update its guidance in November 2024 to address the remaining gaps. Doing so expeditiously would enable lead agencies to use the updated guidance for their required January 2025 Al risk assessments.

_ United States Government Accountability Office