GAO Highlights

Highlights of GAO-24-106246, a report to congressional addressees

Why GAO Did This Study

Executive Order No. 14110, issued in October 2023, notes that while responsible AI use has the potential to help solve urgent challenges and make the world more secure, irresponsible use could exacerbate societal harms and pose risks to national security. Consistent with requirements of Executive Order No. 13960, issued in 2020, DHS has maintained an inventory of its AI use cases since 2022.

This report examines the extent to which DHS (1) verified the accuracy of its inventory of AI systems for cybersecurity and (2) incorporated selected practices from GAO's AI Accountability Framework to manage and oversee its use of AI for cybersecurity.

GAO reviewed relevant laws, OMB guidance, and agency documents, and interviewed DHS officials. GAO applied 11 key practices from the Framework to DHS's AI cybersecurity use case—Automated PII Detection. DHS uses this tool to prevent unnecessary sharing of PII. GAO selected the 11 key practices to reflect all four Framework principles, align with early stages of AI adoption, and be highly relevant to the specific use case.

What GAO Recommends

GAO is making eight recommendations to DHS, including that it (1) expand its review process to include steps to verify the accuracy of its AI inventory submissions, and (2) fully implement key AI Framework practices such as documenting sources and ensuring the reliability of the data used. DHS concurred with the eight recommendations.

View GAO-24-106246. For more information, contact Candice N. Wright at (202) 512-6888 or wrightc@gao.gov or Kevin Walsh at (202) 512-6151 or walshk@gao.gov.

February 2024

ARTIFICIAL INTELLIGENCE

Fully Implementing Key Practices Could Help DHS Ensure Responsible Use for Cybersecurity

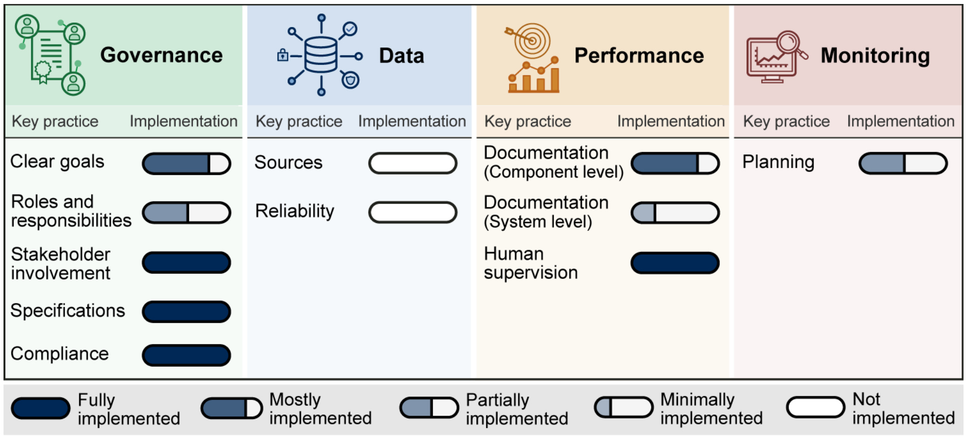
What GAO Found

To promote transparency and inform the public about how artificial intelligence (AI) is being used, federal agencies are required by Executive Order No. 13960 to maintain an inventory of AI use cases. The Department of Homeland Security (DHS) has established such an inventory, which is posted on the Department's website.

However, DHS's inventory of AI systems for cybersecurity is not accurate. Specifically, the inventory identified two AI cybersecurity use cases, but officials told us one of these two was incorrectly characterized as AI. Although DHS has a process to review use cases before they are added to the AI inventory, the agency acknowledges that it does not confirm whether uses are correctly characterized as AI. Until it expands its process to include such determinations, DHS will be unable to ensure accurate use case reporting.

DHS has implemented some but not all of the key practices from GAO's AI Accountability Framework for managing and overseeing its use of AI for cybersecurity. GAO assessed the one remaining cybersecurity use case known as Automated Personally Identifiable Information (PII) Detection—against 11 AI practices selected from the Framework (see figure).

Status of the Department of Homeland Security's Implementation of Selected Key Practices to Manage and Oversee Artificial Intelligence for Cybersecurity



Governance		Data		Performance		Monitoring	
Key practice	Implementation	Key practice	Implementation	Key practice	Implementation	Key practice	Implementation
Clear goals	◕	Sources	○	Documentation (Component level)	◕	Planning	◑
Roles and responsibilities	◑	Reliability	○	Documentation (System level)	◔		
Stakeholder involvement	●			Human supervision	●		
Specifications	●						
Compliance	●						

● Fully implemented ◕ Mostly implemented ◑ Partially implemented ◔ Minimally implemented ○ Not implemented

Source: GAO analysis of agency documents and interviews with Department of Homeland Security officials; GAO (icons). | GAO-24-106246

GAO found that DHS fully implemented four of the 11 key practices and implemented five others to varying degrees in the areas of governance, performance, and monitoring. It did not implement two practices: documenting the sources and origins of data used to develop the PII detection capabilities, and assessing the reliability of data, according to officials. GAO's AI Framework calls for management to provide reasonable assurance of the quality, reliability, and representativeness of the data used in the application, from its development through operation and maintenance. Addressing data sources and reliability is essential to model accuracy. Fully implementing the key practices can help DHS ensure accountable and responsible use of AI.