GAO@100

Highlights

Highlights of GAO-22-104144, a report to Chair, Subcommittee on Emerging Threats and Spending Oversight, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

It is essential that DHS, its component agencies, and its contractors protect the PII that they collect and maintain. Implementing and enforcing appropriate policies and controls can help prevent improper PII access and use.

GAO was asked to review DHS's policies and procedures for protecting the PII collected by or shared with its contractors. This report discusses the extent to which (1) DHS has developed policies and procedures to mitigate the risks to PII; (2) selected DHS components have provided oversight of privacy controls within contractor-operated systems, and (3) DHS components have ensured that privacy incidents in contractor-operated systems are properly identified and remediated.

GAO analyzed DHS policies and procedures, selected and reviewed six major DHS components, evaluated contractor-operated system documentation related to the oversight of privacy controls, and compared contractor-related privacy incident handling and response activities to DHS requirements. GAO also interviewed relevant officials at DHS and its major components.

What GAO Recommends

GAO is making seven recommendations to DHS components to improve their oversight of contractors' privacy controls and remediation of incidents. DHS concurred with the recommendations and outlined steps planned or taken to address them.

View GAO-22-104144. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

December 2021

DHS PRIVACY

Selected Component Agencies Generally Provided Oversight of Contractors, but Further Actions Are Needed to Address Gaps

What GAO Found

The Department of Homeland Security (DHS) developed policies and procedures to mitigate the risks to personally identifiable information (PII) on contractor-operated IT systems. These policies address federal privacy requirements, standards, and guidelines in the following key areas:

- Establishing and maintaining a comprehensive privacy program.
- Providing agency-wide privacy training for all employees and contractors.
- Overseeing information systems operated by contractors.
- Ensuring implementation of privacy controls for contractor systems.
- Ensuring incident response procedures for contractor systems.

As shown below, selected DHS components addressed most of the key privacy control activities for overseeing contractor-operated systems.

Assessment of Selected DHS Components' Oversight of the Implementation of Privacy Controls in Selected Contractor-Operated Systems

Associated activities	CBP	DHS HQ	FEMA	ICE	TSA	USCG
Establish roles and responsibilities	Met	Met	Met	Met	Met	Met
Define privacy requirements in contracts	Met	Met	Met	Met	Met	Met
Identify and address gaps in privacy compliance	Met	Met	Met	Met	Met	Not met
Develop and implement a comprehensive training policy	Met	Met	Met	Met	Met	Met
Administer annual privacy training and targeted role-based privacy training	Met	Partially met	Met	Met	Met	Partially met
Establish and maintain an inventory of all programs and systems with PII	Met	Met	Met	Met	Met	Met
Provide information to contractors describing PII in their possession	Met	Met	Met	Met	Met	Met
Evaluate any proposed new instances of sharing PII with third parties	Met	Met	Met	Met	Not met	Not met

CBP = U.S. Customs and Border Protection, DHS HQ = Department of Homeland Security headquarters, FEMA = Federal Emergency Management Agency, ICE = Immigration and Customs Enforcement, TSA = Transportation Security Administration, USCG = United States Coast Guard

Met = met associated activities; partially met = partially met associated activities; not met = did not meet associated activities

Source: GAO analysis of agency-provided data.| GAO-22-104144

Although the DHS components complied with most of the requirements, gaps existed. For example, USCG did not demonstrate that it identified and addressed gaps in privacy compliance, DHS HQ did not administer role-based privacy training, and TSA did not demonstrate its evaluation of proposed new instances of PII sharing in contractor-operated systems.

Regarding privacy incidents, DHS developed *Privacy Incident Handling Guidance*, which outlines the department's process for how incidents are to be identified and remediated. Of the four reviewed components that had a breach of data, three fully identified, remediated, and shared lessons learned for the incidents. However, one component did not document all necessary remediation activities. Fully documenting remediation activities helps ensure that all appropriate steps have been taken to lessen potential harm that the loss, compromise, or misuse of PII could have on affected individuals.