



Why This Matters

To protect the Nation's borders and ports of entry, U.S. Customs and Border Protection (CBP) employees, contractors, or partners have access to CBP's operations, systems, and data. Based on job function or role, these trusted insiders are typically given unfettered or elevated access to mission-critical assets.

Trusted insiders could use their access or insider knowledge to exploit CBP's physical and technical vulnerabilities with the intent to cause harm. Types of insider threats could include spying, release of information, sabotage, corruption, impersonation, theft, smuggling, and terrorist attacks.

DHS Response

Our report had four recommendations to improve CBP's insider threat program.

CBP concurred with all of the recommendations.

For Further Information:

Contact our Office of Public Affairs at (202)254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

CBP Has Taken Steps To Address the Insider Threat But Challenges Remain

What We Determined

CBP has made progress in addressing the risk of insider threats across the organization. We determined that CBP established a working group and committee focused on the risk. In addition, CBP researches employee behavior, conducts pre-employment screening including polygraph assessments, and participates in border corruption task forces with the Federal Bureau of Investigation. CBP established a Joint Intake Center and Security Operations Center to centrally identify, monitor, and respond to potential insider threat risks or incidents in information systems and networks.

CBP can improve its insider threat program by:

- 1) Implementing policies and procedures that integrate the requirements, standards, and guidance provided by the administration, Department of Homeland Security (DHS), and the National Institute of Standards and Technology.
- 2) Expand current security and awareness training program to include insider threat-based training for all agency employees.
- 3) Strengthen technical security controls and processes of IT assets and operations including applying critical security patches and preventing use of unauthorized devices and exfiltration of sensitive information.
- 4) Perform periodic onsite assessments of CBP sites to identify unauthorized wireless networks and devices connected to the CBP network.

What We Recommend

We recommend that the Assistant Commissioner and Chief Information Officer Office of Information and Technology for CBP:

- 1) Establish an agency-wide insider threat program responsible for identifying and remediating the risk posed by the insider threat.
- 2) Implement an insider threat training and awareness program for the entire CBP workforce.
- 3) Strengthen technical security controls and processes of IT assets and operations including applying critical security patches and preventing use of unauthorized devices and exfiltration of sensitive information.
- 4) Perform periodic onsite assessments of CBP sites to identify unauthorized wireless networks and devices connected to the CBP network.