U.S. Department of Commerce ★ Office of Inspector General

Report Highlights

BIS Needs to Improve Its Incident Response Capabilities to Handle Sophisticated Cyberattacks

Evaluation Report OIG-25-022-I
June 11, 2025

What We Audited | Our objective was to assess the adequacy of actions taken by the Bureau of Industry and Security (BIS) when detecting and responding to cyber incidents in accordance with federal and departmental requirements.

Why This Matters | Cyberattacks frequently compromise government and business networks. After attackers gain access to a network, they often bypass traditional security measures, leveraging trusted access to compromise sensitive data and systems. Therefore, defending against threats inside the network, such as insider threats, is as crucial as securing its perimeter.

BIS's oversight of export controls helps restrict the proliferation of weapons of mass destruction and the means of delivering them. This makes BIS and the Department attractive targets for sophisticated state-sponsored adversaries.

What We Found | We found that:

- BIS lacked effective detection and response capabilities to handle our simulated malicious activities
- BIS misconfigured critical security controls for its export control networks
- BIS mishandled classified and other privileged credentials

Based on our testing, BIS lacked the capabilities, tools, and procedures necessary to detect and respond to our malicious activities. If BIS does not improve its current capabilities, advanced adversaries could significantly harm sensitive U.S. export control efforts, which in turn affects national security.

What We Recommend | We made 13 recommendations to BIS to increase endpoint and network protection, proactively seek and mitigate threats, establish procedures to respond to incidents, restrict network and user access, and improve the security of network credentials. BIS concurred with our recommendations and is working to implement them.

★ Visit us for more information and to view our other reports: ★