Audit of the Department's Vulnerability Reporting and Resolution Program

Audit Report OIG-26-002-A
November 20, 2025

What We Audited | Our objective was to assess the effectiveness of the Department's program for managing public-reported vulnerabilities in its public-facing information technology systems.

Why This Matters | To foster economic growth and opportunities, the Department relies on internet-accessible systems such as government websites, web and mobile applications, third-party services, and databases, which allow the Department to interact with the public by providing services like weather prediction, processing patent applications, and supplying international trade information. With this public accessibility comes an inherent risk of cyberattacks as internet-accessible systems are exposed to global threats and do not have the full protection of internal network defenses.

Recognizing this inherent risk, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) issued *Develop and Publish a Vulnerability Disclosure Policy*, which states, "[c]ybersecurity is a public good that is strongest when the public is given the ability to contribute." This directive requires that each federal agency establish a vulnerability disclosure policy (VDP) that authorizes members of the public (security researchers) to identify and report vulnerabilities on internet-accessible government systems.

What We Found | The Department established a vulnerability disclosure program; however, it was not fully effective. Specifically, the Department's VDP did not include all internet-accessible systems, the VDP's testing guidelines restricted the tools public security researchers could use to identify system vulnerabilities, the Department did not always fully remediate reported vulnerabilities, and the Department did not always remediate vulnerabilities within established deadlines.

What We Recommend | We made three recommendations to the Department to revise the testing scope to align with CISA's VDP policy, update and implement VDP procedures, and work with bureaus to implement an automated solution to prompt action on delayed vulnerability remediation. The Department concurred with our recommendations and is working to implement them.