Spotlight
Department of Homeland Security
Office of Inspector General
May 2012 OIG-12-83

U. S. Citizenship and Immigration Services' Laptop Safeguards Need Improvements

Why This Matters

U. S. Citizenship and Immigration Services (USCIS) has more than 18,000 employees and contractors working at 250 offices around the world. It uses laptop computers to help fulfill its mission of overseeing lawful immigration to the United States. Additionally, USCIS contractors are issued laptops as government-furnished equipment to access USCIS systems. While the mobility of laptops increases workforce productivity, this same mobility increases the risk of theft and unauthorized data disclosure. The increased risk of theft of laptop computers is associated with both cost and security. For example, when laptops are stolen, there is a security risk of data disclosure.

DHS Response

The Director of USCIS concurred with all five of our recommendations and USCIS will: (1) certify that all equipment is assigned to an end user; (2) standardize the process for recording government-furnished equipment; (3) update current policies and instructions to specifically address laptop security; (4) develop a process to updated non-networked laptops manually, and (5) increase its communications concerning the responsibilities for properly maintaining laptops.

These recommendations are considered resolved, but will remain open until USCIS provides documentation to support that the planned corrective actions are completed.

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

What We Determined

USCIS' laptop controls did not sufficiently safeguard its laptops from loss or theft and did not protect the data on the laptops from disclosure.

Specifically, USCIS did not have an accurate inventory of its laptops as property custodians did not consistently enter laptop data into the property management system, and data in different systems did not always agree. Furthermore, not all laptops were assigned to specific users, and USCIS did not adequately track which laptops were provided to contractors. Finally, USCIS did not enhance physical security controls by providing cables and locks for laptops. These deficiencies increased the risk of loss or theft of USCIS laptops.

We also determined that the USCIS configuration management process for providing software upgrades to its laptop computers needs improvement. Specifically, not all USCIS laptops had the latest encryption software, operating systems, or service packs. Furthermore, not all laptops received technical updates in a 30-day period. These deficiencies increased the risk that identified laptop vulnerabilities would not be resolved in a timely manner.

What We Recommend

We recommended that USCIS take steps to improve its laptop inventory and configuration management processes. Specifically, we recommended that the USCIS Chief Information Officer:

Recommendation #1: Ensure that laptop data are entered consistently into the USCIS property management system.

Recommendation #2: Develop a consistent process to record when laptops are initially provided as government-furnished equipment.

Recommendation #3: Provide appropriate locks and cables for laptops that may not be secured in locked offices in a locked cabinet, or desk when unattended.

Recommendation #4: Ensure that USCIS configuration management software and processes enable the updating of laptops' operating systems and encryption software with the latest releases.

Recommendation #5: Develop procedures to ensure that USCIS assigned laptops are connected to its network for system and software updates on a monthly basis.