

# Spotlight

Department of Homeland Security



## Office of Inspector General

May 2013 OIG-13-93

### Why This Matters

The United States Coast Guard (USCG), one of the five armed forces in the United States and the only military branch within the Department of Homeland Security, has a mission to protect the public, the environment, and our nations' maritime economic interests. To accomplish its mission, USCG personnel use laptop computers to perform their assigned duties while they are working at alternate locations, teleworking, on travel, or on vessels. While the mobility provided by laptop computers increases productivity, their use introduces a greater risk of theft and unauthorized disclosure of sensitive data.

### DHS Response

USCG concurred with all of our recommendations and is taking actions to address these recommendations.

## USCG Must Improve the Security and Strengthen the Management of Its Laptops

### What We Determined

USCG has taken actions to govern, track, and secure its laptops. For example, USCG has deployed a component-wide inventory database to account for its property, including laptops. Additionally, USCG has centralized the configuration and patch management of its standard laptops. USCG has also established policies and procedures for securing standard laptops and defining the authorized use of wireless devices, services, and technologies at the component.

USCG needs to improve its laptop acquisition and inventory management practices and strengthen laptop security controls. Specifically, it needs to improve its laptop recapitalization program to eliminate excess quantities of unused laptops. In addition, it should reduce the acquisition of non-standard laptops, which represent a significant portion of the inventory. Non-standard laptops are acquired outside of the recapitalization program, and generally do not meet USCG security standards. Having large numbers of non-standard laptops that lack adequate security may compromise the integrity and confidentiality of USCG data and systems. Finally, USCG must improve the accountability of its laptop inventory and address deficiencies in implementing required configuration settings, deploying security patches to its laptops timely, and developing and implementing procedures to erase and render sensitive data stored on laptop hard drives unrecoverable.

### What We Recommend

We are making two recommendations to the Assistant Commandant for Planning, Resources, and Procurement to address weaknesses in the review of annual laptop inventory results by USCG Headquarters and the reporting of lost and stolen laptops. We are making five recommendations to the Assistant Commandant for Command, Control, Communications, Computers, and Information Technology to address deficiencies in the procurement and oversight of non-standard laptops, implementation of required configuration settings, timely installation of security patches, and development of procedures for erasing and rendering sensitive data stored on laptop hard drives unrecoverable.

### For Further Information:

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