Spotlight

Department of Homeland Security

Office of Inspector General

June 2012 OIG-12-93

# Progress Has Been Made in Securing Laptops and Wireless Networks at FEMA

## Why This Matters

The Federal Emergency Management Agency (FEMA) coordinates the Federal Government's role in preparing for, preventing, mitigating the effects of, responding to, and recovering from natural or man-made domestic disasters. To accomplish its mission, FEMA relies on the use of laptop computers and wireless technologies. Although the mobility of laptops has increased the productivity of the FEMA workforce, it has also increased the risk of theft and unauthorized disclosure of sensitive data. In addition, wireless technologies can introduce significant security issues when not properly configured.

## DHS Response

FEMA concurs with our recommendations in the above referenced draft report. The Office of the Chief Information Officer has taken actions to address these recommendations. Plans of Action and Milestones are being developed to ensure the recommendations are implemented in a timely manner.

**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

FEMA has taken actions to improve the inventory and configuration management controls to protect its laptop computers and the sensitive information they store and process. Furthermore, FEMA has implemented technical controls to protect the information stored on and processed by its wireless networks and devices.

However, we found weaknesses in the component-wide adoption of FEMA's automated property management system, reporting of lost and stolen laptops, implementation of hard drive encryption, use of a standardized laptop image, timely installation of security patches, documentation of laptop sanitization, and accounting for wireless networks. These weaknesses may put laptops and the sensitive information stored and processed on them at risk of exploitation. Improvements are needed to address security risks and ensure the security of laptops and wireless networks and devices.

## What We Recommend

We are making two recommendations to the Chief Administrative Officer to address the weaknesses in the component-wide adoption of its automated property management system and reporting of lost and stolen laptops. We are making five recommendations to the Chief Information Officer to mitigate deficiencies in the implementation of hard drive encryption, use of a standardized laptop image, timely installation of security patches, documentation of laptop sanitization, and accounting for wireless networks.