Spotlight
Department of Homeland Security
Office of Inspector General
June 2012 OIG-12-88

Why This Matters

Universal Serial Bus (USB) flash drives and other portable devices, such as the Android and Apple based smartphones, and tablets, have become widely used tools for today's mobile workforce. These portable devices allow workers to perform tasks at any time and from any place as well as transport large volume of data efficiently.

While portable devices may improve productivity, they expose the Department to new security risks, such as malware, inadvertently expose classified information or personally identifiable information. The Department must implement controls to mitigate risks associated with the use of portable devices.

DHS Response

The Chief Information Officer (CIO) concurred with all three recommendations.

DHS Needs to Address Portable Device Security Risks

What We Determined

The Department of Homeland Security (DHS) has taken actions to govern, track, categorize, and secure portable devices. Specifically, DHS and its components have developed policies, procedures, and training regarding the use of portable devices. Additionally, some components include portable devices as part of their accountable personal property inventory.

However, DHS still faces challenges in using these devices to carry out its mission and increase the productivity of its employees. For example, components must develop policies and procedures to govern the acceptable use and accountability of portable devices. Further, we determined that unauthorized Universal Serial Bus (USB) devices had been connected to the workstations at selected components. Finally, DHS must implement controls to mitigate the risks associated with the use of portable devices and to protect the sensitive information that these devices stored and process.

What We Recommend

We recommend that the CIO:

1) Coordinate with the Chief Administrative Officer and component CIOs to update their asset management policies to ensure that USB thumb drives are recorded as sensitive personal property. In addition, components should record USB thumb drives as sensitive personal property in their asset management systems.

2) Enhance the Department's annual information technology security awareness training to remind users of their responsibilities, acceptable behaviors, and associated risks when using government issued portable devices.

3) Work with the Immigration and Customs Enforcement CIO to ensure compliance with DHS guidance on authentication requirements for Android and iOS devices.

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