OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

FOR IMMEDIATE RELEASE
Monday, December 22, 2014

For Information Contact:
Public Affairs (202) 254-4100

IT Security Suffers from Noncompliance

The Department of Homeland Security (DHS) has made progress to improve its information security program, but noncompliance by several DHS component agencies is undermining that effort, according to a new report by the DHS Office of Inspector General (OIG).

OIG analysts' Evaluation of DHS' Information Security Program for Fiscal Year 2014 cited a shift to risk-based management of IT security and implementation of an agency-wide performance plan as positive developments. However, the OIG raised concerns over a lack of compliance by components and urged DHS leadership to strengthen its oversight and enforcement of existing security policies. Specifically, the OIG found:

- The United States Secret Service refused to provide DHS' Chief Information Security Officer (CISO) with required data on its systems security, making it extremely difficult for the CISO to determine the agency's performance and compliance with security requirements. The Inspector General sent a memorandum to the Secret Service Acting Director expressing concern over the Component's refusal to comply with mandated computer security policies. In response to the memorandum, the Secret Service signed an agreement with DHS' Chief Information Officer to provide the required data on its systems security now and in the future.

- DHS and its Components are continuing to operate information systems without the proper authority to operate (ATO). For example, the Federal Emergency Management Agency (FEMA) has five "Top Secret" systems that have been operating without ATOs, some of which expired in August 2013. Furthermore, the total number of the Department's "Sensitive But Unclassified" and "Secret" systems without valid ATOs increased from 76 in FY 2012 to 191 in FY 2014. When operating systems without valid ATOs, DHS and its Components cannot ensure that the controls implemented are effective to protect sensitive information stored and processed by the systems.

- FEMA's system inventory fluctuated significantly between October 2013 and July 2014. For example, FEMA reported 85 operational systems in October 2013. However, the number of systems dropped to 84 in January 2014, increased to 109 in April 2014, and then decreased to 91 systems in July 2014. Due to the lag time required to develop or procure a new system, system inventory levels should not fluctuate significantly within a few months. These abnormal fluctuations may indicate that either the Department's inventory methodology is not accurately capturing the number of systems that Components maintain, or

Components are circumventing the Department's capital planning investment process to procure or develop new systems independently.

- Components are not mitigating security vulnerabilities timely, including high-risk vulnerabilities such as Heartbleed. Delays in mitigating security vulnerabilities may have exposed sensitive DHS data to potential exploit.

- FEMA and United States Citizenship and Immigration Service are still using the Microsoft Windows XP operating system, which may be vulnerable to potential exploit. Microsoft stopped providing software updates to mitigate security vulnerabilities on these older systems in April 2014.

The OIG's information security evaluation, required by law to be performed annually, also cited concerns with DHS and Component implementation of IT configuration management, incident response and reporting, specialized training, account and identity management, and contingency planning.

"DHS has worked to improve and secure its vast IT resources," said Inspector General John Roth. "But those improvements can only be effective if component agencies fully adhere to the rules and DHS management vigorously enforces compliance. Failure to do so will pose a serious threat to DHS and its Homeland Security missions."

###