Spotlight

Department of Homeland Security

Office of Inspector General

October 2012 OIG-13-04

Why This Matters

Due to the increasing threat to information systems and the highly networked nature of the Federal computing environment, the Congress, in conjunction with the Office of Management and Budget, requires an annual review and reporting of agencies' compliance with Federal Information Security Management Act (FISMA) requirements. FISMA focuses on the program management, implementation, and evaluation of the security of unclassified and national security systems and requires each Federal agency to develop, document, and implement an agency-wide security program.

DHS Response

DHS concurs with all recommendations referenced in the draft report. The Acting Chief Information Security Officer (CISO) has taken actions to address the recommendations.

For Further Information:

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

Evaluation of DHS' Information Security Program for Fiscal Year 2012

What We Determined

DHS continues to improve and strengthen its security program. During the past year, DHS developed and implemented the Fiscal Year 2012 Information Security Performance Plan to focus on areas that the Department would like to improve upon throughout the year. Specifically, DHS developed several key elements that are indicative of a strong security program. In addition, DHS has taken actions to address the Administration's cybersecurity priorities which include the implementation of trusted internet connections, continuously monitoring the Department's information systems, and employing personal identity verification compliant credentials to improve logical access for its systems.

However, components are still not executing all of the Department's policies, procedures, and practices. For example, systems are being authorized though key information is missing or outdated, Plans of Action and Milestones (POA&M) are not being created for all known information security weaknesses or mitigated in a timely manner, and DHS baseline security configurations are not being implemented for all systems. Additional information security program areas that need improvement include incident detection and analysis, specialized training, account and identity management, and contingency planning. Finally, the Department still needs to (1) consolidate all of its external connections, (2) implement a near real-time monitoring capability, and (3) employ personal identity verification compliant cards for logical access on its information systems.

What We Recommend

We recommend that the Acting CISO:

(1) Establish a process to ensure that United States Government Configuration Baseline settings are implemented and maintained at components.
(2) Strengthen the Information Security Office (ISO) review process to ensure that all applicable controls are included in the security documentation when authorizing systems.
(3) Improve the process to ensure that DHS baseline configuration settings are implemented and maintained on components' information systems. The process should include testing and the use of automated tools and security templates.
(4) Strengthen the ISO review process to ensure that POA&Ms, including those for classified systems, are complete and current.
(5) Enhance the Department's revised role-based training program to ensure that appropriate role-based training is provided to all individuals with significant security responsibilities to perform their required security functions.
(6) Establish a process to ensure that security patches and service packs are applied timely and effective controls are implemented on components' databases and servers.