



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 DHS Chief Information Security Officer has taken actions to address the recommendations.

Evaluation of DHS' Information Security Program for Fiscal Year 2013

What We Determined

DHS continues to improve and strengthen its information security program. During the past year, DHS drafted an ongoing authorization methodology to help improve the security of the Department's information systems through a new risk management approach. Additionally, DHS developed and implemented the Fiscal Year 2013 Information Security Performance Plan which defines the performance requirements, priorities, and overall goals for the Department throughout the year. DHS has also taken actions to address the Administration's cybersecurity priorities, which include the implementation of trusted internet connections, continuous monitoring of the Department's information systems, and strong authentication.

While these efforts have resulted in some improvements, components are still not executing all of the Department's policies, procedures, and practices. Our review identified the following more significant exceptions to a strong and effective information security program: (1) systems are being operated without authority to operate; (2) plans of action and milestones (POA&M) are not being created for all known information security weaknesses or mitigated in a timely manner; and (3) baseline security configuration settings 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.

What We Recommend

We recommend that the DHS Chief Information Security Officer:

- (1) Establish a process to ensure that baseline configuration settings are being implemented and maintained on all workstations and servers, including non Windows platforms.
- (2) Ensure that all operational information systems have current authorization to operate.
- (3) Improve the Information Security Office's POA&M review process to ensure that all POA&Ms, including "Top Secret" systems, are being remediated timely and in compliance with DHS guidance.
- (4) Establish enterprise wide security training requirements to ensure all privileged users receive necessary role-based specialized security training.
- (5) Strengthen the Department's oversight on its "Top Secret" systems by performing critical control reviews on selected systems to ensure the required controls are implemented.

For Further Information:

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