



### Why This Matters

In July 2010, the Office of Management and Budget (OMB) designated the Department of Homeland Security (DHS) with the primary responsibilities of overseeing the Federal government-wide information security program. The National Protection and Programs Directorate (NPPD) is primarily responsible for fulfilling the Department's cybersecurity mission. NPPD's Office of Cybersecurity and Communications (CS&C) assumes DHS' additional cybersecurity responsibilities to manage the Federal Information Security Management Act (FISMA) reporting process and oversee the Trusted Internet Connection initiative.

### DHS Response

The report contains six recommendations aimed at addressing NPPD's implementation of the Department's additional cybersecurity responsibilities to improve the security posture of the Federal Government. NPPD concurred with all recommendations.

### For Further Information:

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

## DHS Can Take Actions To Address Its Additional Cybersecurity Responsibilities

### What We Determined

NPPD has taken actions to improve the information security posture at Federal agencies. For example, the NPPD Federal Network Resilience division takes an active approach towards managing the annual FISMA reporting process. Further, the Federal Network Resilience division conducts information security assessments at selected Federal agencies.

Although actions have been taken, NPPD can make further improvements to address its additional cybersecurity responsibilities. For example, the Federal Network Resilience division must develop a strategic implementation plan that defines its long-term goals on improving agencies' information security programs. Further, increased communication and coordination with Federal agencies can improve the FISMA reporting process. Finally, NPPD must address the deficiencies in maintaining and tracking the training records of its contractor personnel as well as implement the required DHS baseline configuration settings on its application, CyberScope. We made six recommendations aimed at addressing and improving NPPD's implementation of DHS' additional cybersecurity responsibilities.

### What We Recommend

We recommend that the Acting Assistant Secretary, CS&C:

- 1) Coordinate with OMB to develop a strategic implementation plan which identifies long-term goals and milestones for Federal agency FISMA compliance.
- 2) Update and finalize internal operating procedures and guidance documents to ensure that cyber responsibilities and procedures are clearly defined.
- 3) Improve communication and coordination with Federal agencies by providing additional clarity regarding the FISMA reporting metrics.
- 4) Implement a process to analyze and provide detailed feedback to Federal agencies concerning monthly vulnerability data feeds.
- 5) Establish a process to ensure that all CyberScope contractor system administrators have received adequate security training in compliance with applicable DHS, OMB, and National Institute of Standards and Technology guidance.
- 6) Implement all required DHS baseline configuration settings on the CyberScope database.