



Why This Matters

The Comprehensive National Cybersecurity Initiative was established to enable and support shared situational awareness and collaboration across the Federal cyber operations centers that are responsible for carrying out the United States cyber activities. The National Cybersecurity and Communications Integration Center (NCCIC) of the National Protection and Programs Directorate (NPPD) is responsible for integrating cyber threat information from the five Federal cyber operations centers and collaborating with these centers in responding to cyber security incidents that may pose a threat to the Nation.

DHS Response

NPPD concurred with the seven recommendations and is taking actions to address these recommendations.

DHS' Efforts to Coordinate the Activities of Federal Cyber Operations Centers

What We Determined

NPPD has taken actions to coordinate and share vital cyber threat information with the five Federal cyber operations centers. For example, NCCIC, which is the operational arm of the Office of Cybersecurity and Communications (CS&C) has established partnerships with the other centers to coordinate an effective response on cyber incidents. In addition, NCCIC has increased interagency collaboration and communication through the use of liaisons and participating in regular meetings. Finally, NCCIC has issued-- in collaboration with the Federal Bureau of Investigation-- Joint Indicator Bulletins to assist private sector partners in preventing cyber attacks and protecting intellectual property, trade secrets, and sensitive business information from exploitation and theft.

Still, DHS faces challenges in sharing cyber information among the Federal cyber operations centers. Specifically, DHS must procure cyber tools and technologies to improve its situational awareness efforts. In addition, it needs to work with its cyber operations center partners to develop a standard set of cyber incident reporting categories. Further, DHS has to address insufficient staffing levels that may hinder its ability to provide continuous coverage in all mission areas in the operations center, conduct additional technical training needed to improve staff's incident response skills and update its continuity of operations plans.

What We Recommend

We recommend that the Acting Under Secretary, NPPD (1) procure or develop tools and technologies with enhanced incident management and analytical capabilities; (2) collaborate with the Department of Defense and the National Institute of Standards and Technology to develop a standard set of incident categories to ensure information sharing between all Federal cyber operations centers; (3) augment staffing by adding additional staffing to execute its mission to provide full coverage on the operations floor; (4) collaborate with the Office of Intelligence and Analysis management to increase the number of its analysts available for continuous coverage at the NCCIC; (5) revise the training and exercise plan to include the new qualifications and standards to ensure NCCIC personnel receive the proper training, certifications, and qualifications to perform their assigned duties; (6) update the NPPD continuity of operations plan; and (7) finalize CS&C's continuity of operations plan to reflect the current realignment and test the plan to ensure component personnel understand their roles in the event of emergency.

For Further Information:

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