CYBERSECURITY

DHS’s National Integration Center Generally Performs Required Functions but Needs to Evaluate Its Activities More Completely

What GAO Found

The National Cybersecurity and Communications Integration Center (NCCIC) of the Department of Homeland Security (DHS) has taken steps to perform each of its 11 statutorily required cybersecurity functions, such as being a federal civilian interface for sharing cybersecurity-related information with federal and nonfederal entities. It manages several programs that provide data used in developing 43 products and services in support of the functions. The programs include monitoring network traffic entering and exiting federal agency networks and analyzing computer network vulnerabilities and threats. The products and services are provided to its customers in the private sector; federal, state, local, tribal, and territorial government entities; and other partner organizations. For example, NCCIC issues indicator bulletins, which can contain information related to cyber threat indicators, defensive measures, and cybersecurity risks and incidents and help to fulfill its function to coordinate the sharing of such information across the government.

The National Cybersecurity Protection Act also required NCCIC to carry out its functions in accordance with nine implementing principles, to the extent practicable. However, the extent to which NCCIC adhered to the 9 principles when performing the functions is unclear because the center has not yet determined the applicability of the principles to all 11 functions, or established metrics and methods by which to evaluate its performance against the principles. GAO identified instances where NCCIC had implemented its functions in accordance with one or more of the principles. For example, consistent with the principle that it seek and receive appropriate consideration from industry sector-specific, academic, and national laboratory expertise, NCCIC coordinated with contacts from industry, academia, and the national laboratories to develop and disseminate vulnerability alerts. On the other hand, GAO also identified instances where the cybersecurity functions were not performed in accordance with the principles. For example, NCCIC is to provide timely technical assistance, risk management support, and incident response capabilities to federal and nonfederal entities; however, it had not established measures or other procedures for ensuring the timeliness of these assessments. Until NCCIC determines the applicability of the principles to its functions and develops metrics and methods to evaluate its performance against the principles, the center cannot ensure that it is effectively meeting its statutory requirements.

In addition, GAO identified factors that impede NCCIC’s ability to more efficiently perform several of its cybersecurity functions. For example, NCCIC officials were unable to completely track and consolidate cyber incidents reported to the center, thereby inhibiting its ability to coordinate the sharing of information across the government. Similarly, NCCIC may not have ready access to the current contact information for all owners and operators of the most critical cyber-dependent infrastructure assets. This lack could impede timely communication with them in the event of a cyber incident. Until NCCIC takes steps to overcome these impediments, it may not be able to efficiently perform its cybersecurity functions and assist federal and nonfederal entities in identifying cyber-based threats, mitigating vulnerabilities, and managing cyber risks.

What GAO Recommends

GAO recommends nine actions to DHS for enhancing the effectiveness and efficiency of NCCIC, including to determine the applicability of the implementing principles and establish metrics and methods for evaluating performance; and address identified impediments. DHS concurred with GAO’s recommendations.