January 2016

INFORMATION SECURITY

DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System

GAO Highlights

Highlights of GAO-16-294, a report to congressional committees

Why GAO Did This Study

Cyber-based attacks on federal systems continue to increase. GAO has designated information security as a government-wide high-risk area since 1997. This was expanded to include the protection of critical cyber infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015. NCPS is intended to provide DHS with capabilities to detect malicious traffic traversing federal agencies' computer networks, prevent intrusions, and support data analytics and information sharing.

Senate and House reports accompanying the 2014 Consolidated Appropriations Act included provisions for GAO to review the implementation of NCPS. GAO determined the extent to which (1) the system meets stated objectives, (2) DHS has designed requirements for future stages of the system, and (3) federal agencies have adopted the system. To do this, GAO compared NCPS capabilities to leading practices, examined documentation, and interviewed officials at DHS and five selected agencies. This is a public version of a report that GAO issued in November 2015 with limited distribution. Certain information on technical issues has been omitted from this version.

What GAO Recommends

GAO recommends that DHS take nine actions to enhance NCPS's capabilities for meeting its objectives, better define requirements for future capabilities, and develop network routing guidance. DHS concurred with GAO's recommendations.

View GAO-16-294. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov

What GAO Found

The Department of Homeland Security's (DHS) National Cybersecurity Protection System (NCPS) is partially, but not fully, meeting its stated system objectives:

- **Intrusion detection:** NCPS provides DHS with a limited ability to detect potentially malicious activity entering and exiting computer networks at federal agencies. Specifically, NCPS compares network traffic to known patterns of malicious data, or "signatures," but does not detect deviations from predefined baselines of normal network behavior. In addition, NCPS does not monitor several types of network traffic and its "signatures" do not address threats that exploit many common security vulnerabilities and thus may be less effective.
- **Intrusion prevention:** The capability of NCPS to prevent intrusions (e.g., blocking an e-mail determined to be malicious) is limited to the types of network traffic that it monitors. For example, the intrusion prevention function monitors and blocks e-mail. However, it does not address malicious content within web traffic, although DHS plans to deliver this capability in 2016.
- **Analytics:** NCPS supports a variety of data analytical tools, including a centralized platform for aggregating data and a capability for analyzing the characteristics of malicious code. In addition, DHS has further enhancements to this capability planned through 2018.
- **Information sharing:** DHS has yet to develop most of the planned functionality for NCPS's information-sharing capability, and requirements were only recently approved. Moreover, agencies and DHS did not always agree about whether notifications of potentially malicious activity had been sent or received, and agencies had mixed views about the usefulness of these notifications. Further, DHS did not always solicit—and agencies did not always provide—feedback on them.

In addition, while DHS has developed metrics for measuring the performance of NCPS, they do not gauge the quality, accuracy, or effectiveness of the system's intrusion detection and prevention capabilities. As a result, DHS is unable to describe the value provided by NCPS.

Regarding future stages of the system, DHS has identified needs for selected capabilities. However, it had not defined requirements for two capabilities: to detect (1) malware on customer agency internal networks or (2) threats entering and exiting cloud service providers. DHS also has not considered specific vulnerability information for agency information systems in making risk-based decisions about future intrusion prevention capabilities.

Federal agencies have adopted NCPS to varying degrees. The 23 agencies required to implement the intrusion detection capabilities had routed some traffic to NCPS intrusion detection sensors. However, only 5 of the 23 agencies were receiving intrusion prevention services, but DHS was working to overcome policy and implementation challenges. Further, agencies have not taken all the technical steps needed to implement the system, such as ensuring that all network traffic is being routed through NCPS sensors. This occurred in part because DHS has not provided network routing guidance to agencies. As a result, DHS has limited assurance regarding the effectiveness of the system.