July 2011

INFORMATION SECURITY

State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-11-149, a report to congressional requesters

Why GAO Did This Study

The Department of State (State) has implemented a custom application called iPost and a risk scoring program that is intended to provide continuous monitoring capabilities of information security risk to elements of its information technology (IT) infrastructure. Continuous monitoring can facilitate near real-time risk management and represents a significant change in the way information security activities have been conducted in the past. GAO was asked to determine (1) the extent to which State has identified and prioritized risk to the department in its risk scoring program; (2) how agency officials use iPost information to implement security improvements; (3) the controls for ensuring the timeliness, accuracy, and completeness of iPost information; and (4) the benefits and challenges associated with implementing iPost.

To do this, GAO examined program documentation and compared it to relevant guidance, interviewed and surveyed department officials, and analyzed iPost data.

What GAO Recommends

GAO recommends the Secretary of State direct the Chief Information Officer to take a number of actions aimed at improving implementation of iPost. State agreed with two of GAO's recommendations, partially agreed with two, and disagreed with three. GAO continues to believe that its recommendations are valid and appropriate.

View GAO-11-149 or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

State has developed and implemented a risk scoring program that identifies and prioritizes several but not all areas affecting information security risk. Specifically, the scope of iPost's risk scoring program (1) addresses Windows hosts but not other IT assets on its major unclassified network; (2) covers a set of 10 scoring components that includes many, but not all, information system controls that are intended to reduce risk; and (3) assigns a score for each identified security weakness, although State could not demonstrate the extent to which scores are based on risk factors such as threat, impact, or likelihood of occurrence that are specific to its computing environment. As a result, the iPost risk scoring program helps to identify, monitor, and prioritize the mitigation of vulnerabilities and weaknesses for the areas it covers, but it does not provide a complete view of the information security risks to the department.

State officials reported they used iPost to (1) identify, prioritize, and fix Windows vulnerabilities that were reported in iPost and (2) to implement other security improvements at their sites. For example, more than half of the 40 survey respondents said that assigning a numeric score to each vulnerability identified and each component was very or moderately helpful in their efforts to prioritize vulnerability mitigation.

State has implemented several controls aimed at ensuring the timeliness, accuracy, and completeness of iPost information. For example, State employed the use of automated tools and collection schedules that support the frequent collection of monitoring data, which helps to ensure the timeliness of iPost data. State also relies on users to report when inaccurate and incomplete iPost data and scoring are identified, so they may be investigated and corrected as appropriate. Notwithstanding these controls, the timeliness, accuracy, and completeness of iPost data were not always assured. For example, several instances existed where iPost data were not updated as frequently as scheduled, inconsistent, or incomplete. As a result, State may not have reasonable assurance that data within iPost are accurate and complete with which to make risk management decisions.

iPost provides many benefits but also poses challenges for the department. iPost has resulted in improvements to the department's information security by providing more extensive and timely information on vulnerabilities, while also creating an environment where officials are motivated to fix vulnerabilities based on department priorities. However, State has faced, and will continue to face, challenges with the implementation of iPost. These include (1) overcoming limitations and technical issues with data collection tools, (2) identifying and notifying individuals with responsibility for site-level security, (3) implementing configuration management for iPost, (4) adopting a strategy for continuous monitoring of controls, and (5) managing stakeholder expectations for continuous monitoring activities.