United States Government Accountability Office

GAO

Report to Congressional Requesters

July 2011

INFORMATION SECURITY

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

GAO-11-149

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.

Contents

Abbreviations

AD	Active Directory
CIO	chief information officer
CISO	chief information security officer
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
CAESARS	Continuous Asset Evaluation, Situational Awareness, and Risk Scoring
FISMA	Federal Information Security Management Act of 2002
IT	information technology
iPost	iPost Risk Scoring Program
NIST	National Institute of Standards and Technology
SMS	Systems Management Server
SP	Special Publication
State	Department of State

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 8, 2011

The Honorable Joseph I. Lieberman
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Thomas R. Carper
Chairman
The Honorable Scott Brown
Ranking Member
Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security
Committee on Homeland Security and Governmental Affairs
United States Senate

Like other federal agencies, the Department of State (State) is increasingly dependent upon information technology (IT) and associated services to support functions critical to the department's mission. At the same time, cyber-based threats to federal IT systems and infrastructure are evolving and growing and come from a variety of sources including foreign nations, criminals, terrorists, and disgruntled insiders. The dynamic nature of cyber-based threats and the inevitable changes that occur in federal computing environments underscore the need for developing new capabilities to provide closer to real-time awareness of the security status of federal information systems that support mission critical functions, protect assets, and deliver essential services to constituents.

To accomplish such awareness, State has been at the forefront of federal efforts in developing and implementing a continuous monitoring capability. It has developed and implemented a custom application called iPost that is intended to provide continuous monitoring capabilities over selected elements of State's IT environment. Using data collected by various automated monitoring and management tools and a scoring method based on the premise that higher scores mean higher risk, the iPost risk scoring program is intended to provide local administrators and enterprise-level management with an improved capability to monitor and report on risks and risk mitigation efforts affecting the department's IT infrastructure.

You asked us to review the efficiency and effectiveness of the iPost risk scoring program. Specifically, our objectives were 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.

We conducted our review in the Washington, D.C., metropolitan area, where we obtained and analyzed program documentation, reports, and other artifacts, and interviewed department officials. We compared department documentation with State policies and requirements and relevant National Institute of Standards and Technology (NIST) guidance on risk management and vulnerability scoring. In addition, we developed a survey instrument to obtain information from domestic and overseas department officials on how they used iPost at their sites and descriptions of their experience using it. We also analyzed the timeliness, accuracy, and completeness of iPost data for selected State sites.

We conducted this performance audit from March 2010 to July 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Further details of our objectives, scope, and methodology are included in appendix I.

Background

Information security is a critical consideration for any organization reliant on IT and especially important for government agencies, where maintaining the public's trust is essential. The Federal Information Security Management Act of 2002 (FISMA) established a framework designed to ensure the effectiveness of security controls over information resources that support federal operations and assets. According to FISMA, each agency is responsible, among other things, for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. Consistent with its statutory responsibilities under FISMA, in February 2010, NIST issued Special

Publication (SP) 800-37[1] on implementing effective risk management[2] processes to (1) build information security capabilities into information systems through the application of management, operational, and technical security controls; (2) maintain awareness of the security state of information systems on an ongoing basis though enhanced monitoring processes; and (3) provide essential information to senior leaders to facilitate system authorization decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the nation arising from the operation and use of information systems.

According to NIST guidance these risk management processes:

- promote the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes;
- encourage the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions;
- integrate information security into the enterprise architecture and system development life cycle;
- provide emphasis on the selection, implementation, assessment, and monitoring of security controls, and the authorization of information systems;
- link risk management processes at the information system level to risk management processes at the organization level through a risk executive (function); and
- establish responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems (i.e., common controls).

[1]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Special Publication 800-37 (Gaithersburg, Md.: February 2010).

[2]According to NIST, risk management is a process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability and protect the IT systems and data that support their organizations' missions.

Continuous monitoring of security controls employed within or inherited by the system is an important aspect of managing risk to information from the operation and use of information systems.[3] Conducting a thorough point-in-time assessment of the deployed security controls is a necessary but not sufficient practice to demonstrate security due diligence. An effective organizational information security program also includes a rigorous continuous monitoring program integrated into the system development life cycle. The objective of continuous monitoring is to determine if the set of deployed security controls continue to be effective over time in light of the inevitable changes that occur. Such monitoring is intended to assist maintaining an ongoing awareness of information security, vulnerabilities,[4] and threats[5] to support organizational risk management decisions. The monitoring of security controls using automated support tools facilitates near real-time risk management. As described in the draft NIST SP 800-137,[6] the monitoring process consists of the following various steps:

- defining a strategy;
- establishing measures and metrics;
- establishing monitoring and assessment frequencies;
- implementing the monitoring program;
- analyzing security-related information and reporting findings;
- responding with mitigation actions or rejecting, avoiding, transferring, or accepting risk; and

[3]According to NIST, the term "continuous" in this context means that security controls and organizational risks are assessed, analyzed, and reported at a frequency sufficient to support risk-based security decisions as needed to adequately protect organization information.

[4]A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

[5]A threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, modification of information, and/or denial of service. Threats to information and information systems include environmental disruptions, human or machine errors, and purposeful attacks.

[6]NIST, *Information Security Continuous Monitoring for Federal Information Systems and Organizations (Draft),* Special Publication 800-137 (Gaithersburg, Md.: December 2010).

- reviewing and updating the monitoring strategy and program.

In its September 2010 report, Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) Reference Architecture Report,[7] the Department of Homeland Security (DHS) indicates that a key aspect of a continuous monitoring process is analyzing security-related information, defining and calculating risk, and assigning scores. The report notes that risk scoring can provide information at the right level of detail so that managers and system administrators can understand (1) the state of the IT systems for which they are responsible, (2) the specific gaps between actual and desired states of security protections, and (3) the numerical value of every remediation action that can be taken to close the gaps. This information should help enable responsible managers to identify actions that can add value to improving security. The report also notes that risk scoring is not a substitute for other essential operational and management controls, such as incident response, contingency planning, and personnel security. When used in conjunction with other sources of information, such as the Federal Information Processing Standards 199[8] security categorization and automated asset data repository and configuration management tools, risk scoring can be an important contributor to an overall risk management strategy.

NIST is in the process of developing guidance[9] that extends the CAESARS framework provided by DHS. NIST's extension is to provide information on an enterprise continuous monitoring technical reference architecture to enable organizations to aggregate collected data from security tools, analyze the data, perform scoring, enable user queries, and provide overall situational awareness.

[7]Department of Homeland Security, *Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report* (CAESARS), No. MP100146 (Washington, D.C.: September 2010).

[8]The Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems*, lays out standards for categorizing federal information and information systems as either low impact, moderate impact, or high impact according to the potential impact to an agency should events occur that jeopardize the information and information systems needed by the organization to accomplish its mission.

[9]NIST,*CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture (Draft),* Interagency Report 7756 (Gaithersburg, Md.: February 2011).

NIST has also emphasized the value of planning, scheduling, and conducting assessments of controls as part of a continuous monitoring program in SP 800-37. This program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions or business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system.

State Leads U.S. Diplomatic Efforts around the World

State's key missions are to (1) strive to build and maintain strong bilateral and multilateral relationships with other nations and international organizations; (2) protect the nation against the transnational dangers and enduring threats arising from tyranny, poverty, and disease, global terrorism, international crime, and the spread of weapons of mass destruction; and (3) combine diplomatic skills and development assistance to foster a more democratic and prosperous world integrated into the global economy.

To accomplish its missions, State operates more than 260 embassies, consulates, and other posts worldwide. In addition, the department operates 6,000 passport facilities nationwide, 17 domestic passport agencies, 2 foreign press centers, 1 reception center, 5 offices that provide logistics support for overseas operations, 20 security offices, and 2 financial service centers. State is organized into nine functional bureaus: the Bureaus of Administration, Consular Affairs, Diplomatic Security, Resource Management, Human Resources, Information Resource Management, and Overseas Buildings Operations; the Office of the Legal Adviser; and the Foreign Service Institute. Among other things, these functional bureaus provide services such as policy guidance, program management, and administrative support. In addition, State has six regional, or geographic bureaus including the Bureau of African Affairs, East Asian and Pacific Affairs, European and Eurasian Affairs, Western Hemisphere Affairs, Near Eastern Affairs, and South Asian Affairs. These bureaus focus on U.S. foreign policy and relations with countries within their geographical areas.

State Relies on IT to Support Its Mission

State's IT infrastructure, encompassing its worldwide computer and communications networks and services, plays a critical role in supporting the department's missions. This includes OpenNet—the department's global unclassified network that uses Internet protocol to link State's domestic and local area networks abroad. OpenNet serves both foreign

and domestic locations, has tens of thousands of hosts,[10] and about 5,000 routers and switches. The department budget for IT was approximately $1.2 billion for fiscal year 2010.

The department's Foreign Affairs Manual[11] assigns the following roles and responsibilities for IT to the Bureau of Information Resource Management and Bureau of Diplomatic Security:

- The Bureau of Information Resource Management, headed by the Chief Information Officer (CIO), is to support the effective and efficient creation, collection, processing, transmission, dissemination, storage, and disposition of information required to formulate and execute U.S. foreign policy and manage the department's daily operations. To meet the challenges of providing information in such an environment, the bureau relies on IT to disseminate this information throughout the foreign affairs community.
- The Bureau of Diplomatic Security has global responsibilities, with protection of people, information, and property. Overseas, the bureau implements security programs to ensure the safety of those who work in every U.S. diplomatic mission. In the U.S., the bureau protects the Secretary of State, the U.S. Ambassador to the United Nations, and foreign dignitaries who visit the United States. It also investigates passport and visa fraud, conducts personnel security investigations, and issues security clearances. Additional IT-relevant functions it performs are network monitoring and intrusion detection, incident handling and response, and threat analysis.

The Foreign Affairs Manual also assigns roles and responsibilities to various department officials for information security. These roles and responsibilities are summarized in the following table.

[10]A host refers to a computer that is connected to a network.

[11]The Foreign Affairs Manual outlines the organizational responsibilities and authorities assigned to each major component within State. Volume 5 of the manual identifies the officials responsible for development, oversight, and implementation of the department's IT program and activities, as well as the guidance, standards, and requirements officials are expected to follow when undertaking their responsibilities.

Table 1: Roles and Responsibilities for Information Security at State

Role	Responsibility
Chief Information Officer	Serves as the designated accrediting authority[a] for non-Special Compartmented Information systems, and ensures the availability of State's IT systems and operations to support the department's diplomatic, consular, and management operations.
Chief Information Security Officer (CISO)	Develops and maintains the department's information security program, and coordinates the design and implementation of processes and practices that assess and quantify risk.
Information Management Officer/Information Systems Officer/Systems Administrator	Develops and maintains system security plans for all IT systems and major applications for which they are responsible and participates in risk assessments to periodically reevaluate the sensitivity of the system, risk, and mitigation strategies.
Information Systems Security Officer	Ensures systems are configured, operated, maintained, and disposed of in accordance with all relevant State security guidelines; plays a leading role in introducing an appropriate methodology to help identify, evaluate, and minimize risks to all IT systems; and is responsible to the CISO to ensure the IT system is configured and maintained securely throughout its lifecycle.

Source: State.

[a]A designated accrediting authority or authorizing official is a senior management official or executive with the authority to formally authorize the operation of an information system and accept responsibility for operating the system at an acceptable level of risk to department operations, assets, or individuals.

State Has Implemented iPost and Risk Scoring Program to Monitor and Report on IT Security Weaknesses

State has developed and implemented a complex, custom-made application called iPost to provide an enhanced monitoring capability for its extensive and worldwide IT infrastructure. The source data for iPost come from a variety of enterprise management and monitoring tools including Active Directory (AD), Systems Management Server (SMS), and diagnostic scanning tools. These tools provide vulnerability data, security compliance data, anti-virus signature file data, and other system and network data to iPost. The data are posted to an iPost database, reformatted and reconciled, and then populated into other iPost databases. Data are associated with a "site" or "operational unit,"[12] and integrated into a single user interface portal (or dashboard) that facilitates

[12]Sites, or operational units, within iPost are either identified based on physical location, such as an overseas embassy or domestic facility within the United States, or can be grouped by administrative responsibility or function, such as all hosts within a particular bureau. State also created virtual "unassigned" sites in iPost for hosts for which responsibility was not determined.

monitoring by department users. The primary users of iPost include local and enterprise IT administrators and their management.

Designed specifically for State, iPost provides summary and detailed data as well as the capability to generate reports based on these data. Summary information provides an overview of the current status of hosts at a site, including summary statistics and network activity information. Detailed data on hosts within a site are also available through the application navigation. For example, when looking at data about a specific patch, a user can see which hosts need that patch. Users can select a specific host within the scope of their control to view all the current data iPost has for that host, such as all identified vulnerabilities. Examples of key iPost screens and reports for sites are provided in appendix II.

Implementation of Risk Scoring Program Is to Support Continuous Risk Monitoring

State also developed and incorporated a risk scoring program into iPost that is intended to provide a continuous risk monitoring capability over its Windows-based hosts on the OpenNet network at domestic and overseas locations. The program uses data integrated into iPost from several monitoring tools to produce what is intended to be a single holistic view of technical vulnerabilities. The objectives of the program are to measure risk in multiple areas, motivate administrators to reduce risk, measure improvement, and provide a single score for each host, site, and the enterprise.

Each host and user account is scored in multiple areas known as scoring components. The scoring program assigns a score to each vulnerability, weakness, or other infrastructure issue identified for the host based on the premise that a higher score means higher risk. Thus, the score for a host is the total of the scores of all its weaknesses. Scores are then aggregated across components to give a total or "raw" risk score for each host, site, region, or the enterprise. Scores are "normalized" so that small and large sites can be equitably compared.[13] Letter grades ("A" through "F"), based on normalized scores, are provided to both administrators and senior management with the intent of encouraging risk reduction. The scoring program also has an "exception" process that aims to

[13]The "normalization" of scores involves the calculation of average scores using the number of hosts as the denominator. Thus, the average score for an aggregate (i.e., component, host, site, or enterprise) is equal to the aggregate raw score divided by the aggregate number of hosts or equivalently, the sum of the average scores of its components.

accommodate anomaly situations where the risk cannot be reduced by local administrators because of technical or organizational impediments beyond local control. In such cases, the risk score is to be transferred to the site or operational unit that has responsibility for mitigating the weakness and local administrators are left to address only those weaknesses within their control.

According to a State official, summary data (scores by site and component) are permanently retained in a database while detailed data were generally retained until replaced by updated data from a recent scan. In instances when a host is missed on a scan, the older detailed data are kept until they are judged to be too old to be useful. After that, the host is scored for nonreporting, and the older data are deleted. The official also noted that under a new policy being implemented, detailed data will be retained for two to three scans so that users at a site can see what changed.

State Has Been Recognized for Its iPost Risk Scoring Program

State has been recognized as a leader in federal efforts to develop and implement a continuous risk monitoring capability. In its CAESARS reference architecture report, DHS recognized State as a leading federal agency and noted that DHS's proposed target-state reference architecture for security posture monitoring and risk scoring is based, in part, on the work of State's security risk scoring program. In addition, in 2009 the National Security Agency presented an organizational achievement award to State's Site Risk Scoring Program team for significantly contributing to the field of information security and the security of the nation.

Although iPost Does Not Provide a Complete View of Information Security Risks, It Helps to Prioritize Vulnerability Mitigation Efforts

The iPost risk scoring program identifies and prioritizes several but not all areas affecting information security risk to State's IT infrastructure. Specifically, the scope of the iPost risk scoring program:

- addresses Windows hosts but not other IT assets on the OpenNet network, such as routers and switches;
- covers a set of 10 scoring components that includes several but not all information system controls that are intended to reduce risk; and
- assigns a score for each identified security weakness, but the extent to which the score reflects risk factors such as the impact and likelihood of threat occurrence that are specific to State's computing environment could not be demonstrated.

As a result, the iPost risk scoring program helps to identify, monitor, and prioritize 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.

iPost Risk Scoring Program Only Addresses Windows Host Computers on the OpenNet Network

The scope of State's risk scoring program covers hosts that use Windows operating systems, are members of AD, and are attached to the department's OpenNet network. This includes approximately tens of thousands workstations and servers at foreign and domestic locations.

However, the program's scope does not include other devices attached to the network such as those that use non-Windows operating systems, firewalls, routers, switches, mainframes, databases, and intrusion detection devices. Vulnerabilities in controls for these devices could introduce risk to the Windows hosts and the information the hosts contain or process. State officials indicated that the focus on Windows hosts for risk scoring was due, in part, because of the desire to demonstrate success of the risk scoring program before considering other types of network devices. Windows servers and workstations also comprised a majority of the devices attached to the network and the availability of Microsoft tools such as AD and SMS and other enterprise management tools facilitated the collection of source data from Windows hosts. State officials indicated they were considering expanding the program to include scoring other devices on OpenNet.

iPost's Risk Scoring Program Addresses Several but Not All Information System Controls

In applying the risk management framework to federal information systems, agencies select, tailor, and supplement a set of baseline security controls using the procedures and catalogue of security controls identified in NIST SP 800-53, rev. 3. The effective implementation of these controls is intended to cost-effectively mitigate risk while complying with security requirements defined by applicable laws, directives, policies, standards, and regulations. To ensure that the set of deployed security controls continues to be effective over time in light of inevitable changes that occur, NIST SP 800-37 states that agencies should assess and monitor a subset of security controls including technical, management, and operational controls on an ongoing basis during continuous monitoring.

Using data integrated into iPost from multiple monitoring tools that identify and assess the status of security-related attributes and control settings, the iPost risk scoring program supports a capability to assess and monitor

a subset of the security controls including technical and operational controls on an ongoing basis. The program is built on a set of 10 scoring components, each of which, according to iPost documentation, represents an area of risk for which measurement data were readily available. The program addresses vulnerabilities, security weaknesses, and other control issues affecting risk to the Windows hosts. The 10 scoring components in iPost are described in the following table.

Table 2: Scoring Components of State's Risk Scoring Program

Scoring component	What is scored	Source
1. Vulnerability	Vulnerabilities detected on a host	Scanning tool
2. Patch	Incompletely installed or uninstalled patches required by a host	SMS
3. Security compliance	Failures of a host to use required security settings	Scanning tool
4. Anti-virus	Out-of-date anti-virus signature file	SMS
5. Standard operating environment compliance	Incomplete/invalid installations of any product in the Standard Operating Environment suite, of which there were 19 products	SMS
6. AD users	User account password ages exceeding 60-day threshold (scores each user account, not each host)	AD
7. AD computers	Computer account password ages exceeding 30-day threshold	AD
8. SMS reporting	SMS client agent on host is not reporting all expected information and the incomplete reporting is due to specific type of errors	SMS
9. Vulnerability reporting	Hosts that miss two consecutive vulnerability scans	Scanning tool
10. Security compliance reporting	Hosts that miss two consecutive security compliance scans	Scanning tool

Source: GAO analysis of State data.

Although iPost provides a capability to monitor several types of security controls on an ongoing basis, it did not address other controls intended to reduce risk to Windows hosts, thereby providing an incomplete view of such risk. These controls include physical and environmental protection, contingency planning, and personnel security. Vulnerabilities in these controls could introduce risk to the department's Windows hosts on OpenNet. State officials recognized that these controls and associated vulnerabilities were not addressed in iPost and stated that when they were first developing iPost, they focused on controls and vulnerabilities that could be monitored with existing automated tools such as a scanning tool, AD, and SMS since these could be implemented immediately. State officials believed this approach allowed them to develop a continuous monitoring application in the time frame they did with the limited resources available. Department officials also advised that the scoring program is intended to be scalable to address additional controls and they may add other control areas in the future.

State Could Not Demonstrate the Extent to Which iPost Assigns Scores for Security Weaknesses Based on Risk Factors Specific to Its Computing Environment

According to NIST SP 800-37, risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (1) the adverse impacts[14] that would arise if the circumstance or event occurs and (2) the likelihood of occurrence. In information assurance risk analysis, the likelihood of occurrence is a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability. According to iPost documentation, a key objective of the risk scoring program is to measure risk in multiple areas.

State could not demonstrate the extent to which it considered factors relating to threat, impact, and likelihood of occurrence in assigning risk scores for security weaknesses. In developing the scoring methods for the 10 scoring components, the department utilized a working group comprised of staff from the Bureaus of Information Resource Management and Diplomatic Security. While documentation was limited to descriptions of the certain scoring calculations assigned to each component, State officials explained that working groups comprised of staff from the Bureaus of Information Resource Management and Diplomatic Security had discussions to determine a range of scores for each component. State officials explained that the premise for the scoring method was the greater the risk, the higher the score, and therefore, the greater the priority for mitigation. However, minutes of the working groups' meetings and other documents did not show the extent to which threats, the potential impacts of the threats, and likelihood of occurrence were considered in developing the risk scores and State officials acknowledged these factors were not fully considered. Table 3 provides a description of how State calculates a score for each component.

[14]Impact is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure, modification, or destruction of information or loss of information or information system availability.

Table 3: iPost Component Scoring Methodology as of August 2010

Component	How score is calculated for a host
1. Vulnerability	Sum of vulnerability scores of all detected vulnerabilities. Scores for individual vulnerabilities range from 0.01 and .1 for the lowest-risk vulnerability to 10 for the highest-risk vulnerability.
2. Patch	Sum of patch scores of all incompletely installed patches. Each patch is assigned a score based on its risk level: low = 3, medium = 6, high = 9, and critical = 10.
3. Security compliance	Sum of all scores of all failed security compliance checks. According to one screen, the scores can range from .43 to .9 for each instance of security noncompliance.[a]
4. Anti-virus	After a grace period of 6 days, a score of 6 per day is assigned to a host with an old anti-virus signature file.
5. Standard operating environment compliance	Score of 5 assigned for each missing or unapproved version of a standard application.
6. AD users	Score of 1 assigned for each day an account that does not require a smart-card, and are not disabled or expired, and whose password age exceeds 60 days. Accounts that have no date in AD for the last password reset are assigned a fixed score of 200. If the password is set to never expire, an additional score of 5 is assigned.
7. AD computers	Score of 1 assigned for each day password age exceeds 35 days.[b]
8. SMS reporting	One hundred plus 10 for each day since last day agent correctly reported. Before scoring begins, there is a grace period that varies from 5 to 30 days, depending on the error conditions detected.
9. Vulnerability reporting	After a host has not been scanned in 15 consecutive days, a score of 5 is assigned, then increased at the rate of 1 for each additional 7 days.
10. Security compliance reporting	After a host has not been scanned for 30 consecutive days, a score of 5 is assigned, then increased at the rate of 1 for each additional 15 days.

Source: GAO analysis of iPost documentation.

Note: Numeric scores reflected in the table were displayed in iPost as of August 31, 2010.

[a]Documentation provided by State showed different ranges of scores. For example, another screen displayed in iPost indicated that the scores for security compliance can range from .862 to 4.31. The iPost risk scoring methodology guide dated August 2010 indicates security compliance scores range from .006 to .8.

[b]The iPost risk scoring methodology guide dated August 2010 indicates a score is assigned for each day the password age exceeds 30 days.

The methodology used to assign scores for the vulnerability component illustrates the limits that risk factors such as the impact and likelihood of threats specific to State's environment were considered. Each vulnerability is initially assigned a score according to the Common Vulnerability Scoring System (CVSS). According to NIST guidance,[15]

[15]NIST, *The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems,* Interagency Report 7435 (Gaithersburg, Md.: August 2007).

agencies can use the CVSS base scores[16] stored in the National Vulnerability Database to quickly determine the severity of identified vulnerabilities. Although not required, agencies can then refine base scores by assigning values to the temporal[17] and environmental[18] metrics in order to provide additional contextual information that more accurately reflects the risk to their unique environment. However, State did not refine the base scores to reflect the unique characteristics of its environment. Instead, it applied a mathematical formula to the base scores to provide greater separation between the scores for higher-risk vulnerabilities and the scores for lower-risk vulnerabilities. As a result, the scores may not fully or accurately reflect the risks to State's OpenNet network. Although the iPost risk scoring program does not provide a complete view of the information security risks to the department, it helps to identify, monitor, and prioritize mitigation of vulnerabilities and weaknesses associated with Windows hosts on the OpenNet network.

State Uses iPost to Identify, Prioritize, and Implement Improvements on Windows Hosts

State officials surveyed responded that they used iPost to (1) identify, prioritize, and fix security weaknesses and vulnerabilities on Windows devices and (2) implement other security improvements at their sites. For example, at least half of the respondents said that assigning a numeric score to each vulnerability identified and each component was very helpful with prioritizing their efforts to prioritize the mitigation of Windows vulnerabilities. State officials stated that iPost was particularly helpful because prior to iPost, officials did not have access to tools with these capabilities. However, State officials did not use iPost results to update key security documents related to the assessment and authorization of the OpenNet network.

[16]The base group of metrics reflects the intrinsic and fundamental characteristics of a vulnerability that are constant over time and across user environments, such as how the vulnerability is exploited (locally or remotely) or how complex the attack must be to exploit the vulnerability once system access has been gained—factors that contribute to the likelihood of occurrence. The base group metrics also measure the impact to confidentiality, integrity, and availability of a successfully exploited vulnerability.

[17]The temporal group of metrics reflects the characteristics of a vulnerability that change over time, including the current state of the exploit techniques or code availability, and whether remediation is available to fix the vulnerability.

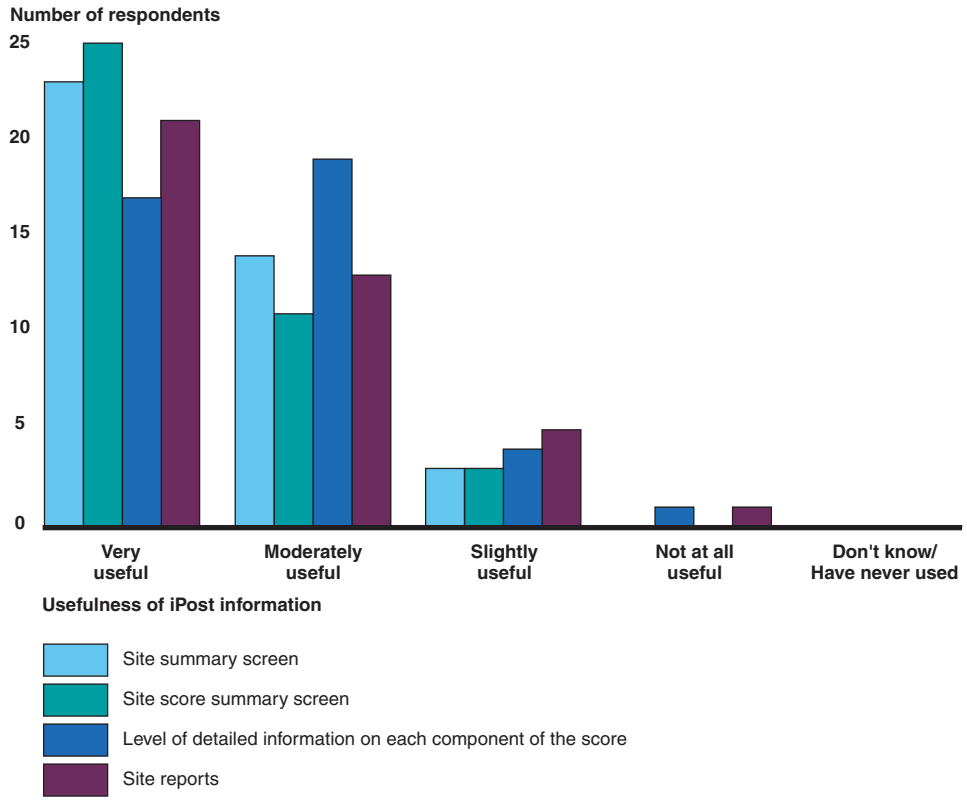
[18]The environmental group of metrics provides the score actually needed for risk prioritization as it pertains to the user's environment. The environmental metrics are specified by users because users are best able to assess the potential impact of a vulnerability within their own environments.

State Officials Primarily Identify, Prioritize, and Fix Weaknesses on Windows Hosts

State officials reported they used iPost to help them to: (1) identify Windows vulnerabilities on the devices for which they were responsible, (2) prioritize the mitigation of vulnerabilities identified, and (3) fix the vulnerability and confirm mitigation was successfully implemented. Specifically, as part of their duties, State officials indicated they reviewed iPost regularly to see the results of the automated scanning of devices at their sites to see what vulnerabilities had been identified. In particular, 14 of 40 survey respondents stated that they viewed the information in iPost at least once per day, 17 viewed information in iPost at least once a week, 3 viewed information at least once a month, and 4 respondents viewed information less than once per month. In addition, State officials we interviewed indicated they reviewed iPost information on a daily basis, with one official stating it was his first task in the morning.

Of the information available in iPost, State officials surveyed noted that some screens and information were particularly useful at their sites. Specifically, the majority of the 40 survey respondents reported that the site summary screen, site score summary screen, level of detailed information on each component, and site reports were very or moderately useful (see fig. 1). These screens show site and host identifying information, statistical data, and graphical representations of the site's risk scores, host computers, accounts, and identified weaknesses for each of the 10 components. Appendix II shows sample screens containing this information.

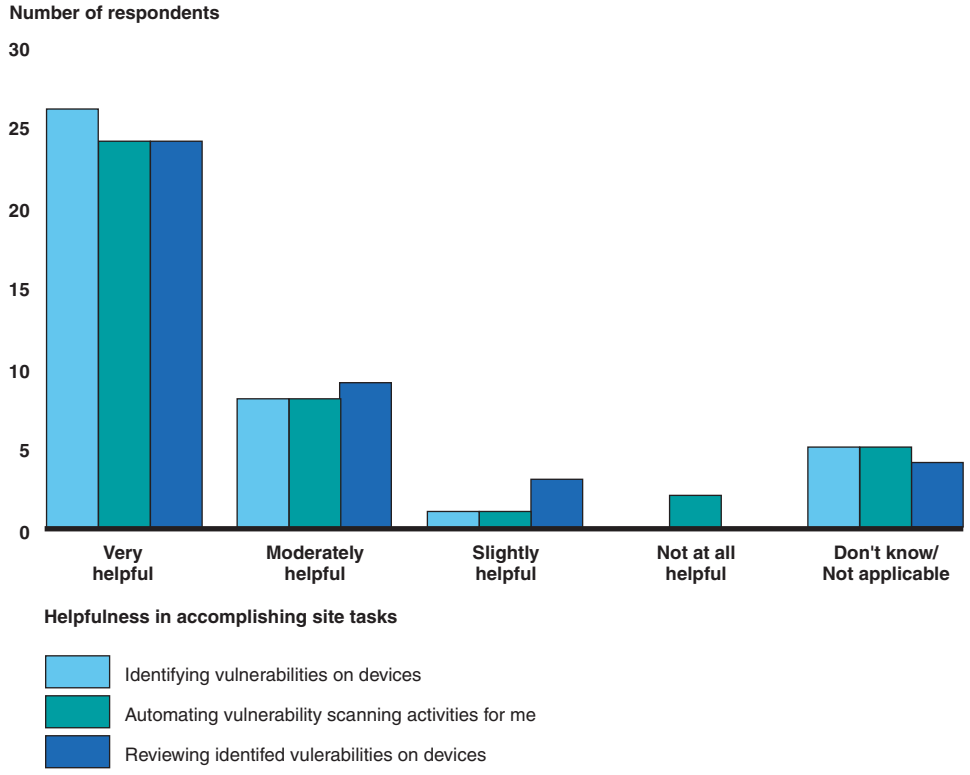
Figure 1: Usefulness of iPost Information



Source: GAO survey of State officials.

The majority of State officials surveyed also indicated that iPost was very helpful in identifying Windows vulnerabilities. In particular, the majority of the 40 survey respondents indicated that iPost was very or moderately helpful in identifying vulnerabilities on devices, providing automated scanning of devices onsite for vulnerabilities, and reviewing identified vulnerabilities on devices (see fig. 2).

Figure 2: Helpfulness of iPost in Accomplishing Site Tasks



Source: GAO survey of State officials.

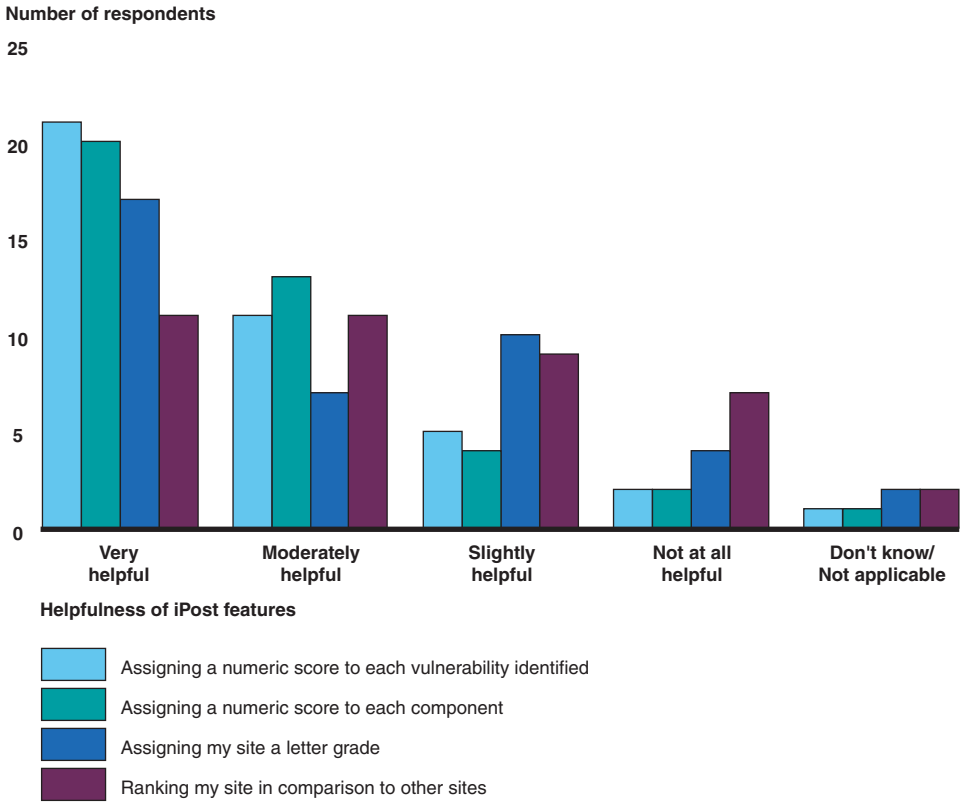
Furthermore, survey respondents and State officials we interviewed also reported being able to identify additional site vulnerabilities at their sites not scored in iPost. For example, one official we spoke to said she would receive incident notices and would use iPost to obtain more information about the incident. Another official noted that iPost helped identify users who were utilizing the most bandwidth on the network. Generally, State officials concluded that iPost was particularly helpful because (1) it provided several officials access to tools with these capabilities they did not have prior to its use and (2) it streamlined the number of software utility and scanning tools officials could use, making the monitoring process more efficient and effective.

Risk Scoring Features Help Officials Prioritize Vulnerability Mitigation

State officials reported that the iPost features helped them prioritize the mitigation of vulnerabilities at their sites. Most survey respondents indicated that iPost was very or moderately helpful with prioritizing the mitigation of Windows vulnerabilities. For example, more than half of the

40 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. In addition, over half of the 40 respondents felt that assigning letter grades to sites was very or moderately helpful in prioritization efforts, though 10 respondents felt this was only slightly helpful, and 4 respondents felt this was not helpful at all. Of the features presented in iPost that assist in prioritization, responses were mixed regarding how helpful ranking of sites in comparison to other sites was for prioritizing vulnerability mitigation, with 22 respondents reporting it was very or moderately helpful, 9 slightly helpful, and 7 not at all helpful. Figure 3 provides details of survey responses.

Figure 3: Helpfulness of iPost Features with Prioritizing Vulnerability Mitigation



Source: GAO survey of State officials.

State officials we interviewed also indicated that iPost assisted them in prioritizing vulnerability mitigation. In particular, they found that scoring the vulnerabilities helped them to identify which ones were necessary to fix first. In regards to the letter grades and ranking, a State official told us the letter grades were useful because they aided him in deciding whether he should fix vulnerabilities identified in iPost (if he/she had a grade lower than an A) or focus on other activities.

iPost Resources Help Officials Fix Vulnerabilities and Confirm Successful Implementation

The iPost dashboard also provides links to available resources that users can utilize to fix identified vulnerabilities. Table 4 provides an overview of available resource links located in iPost.

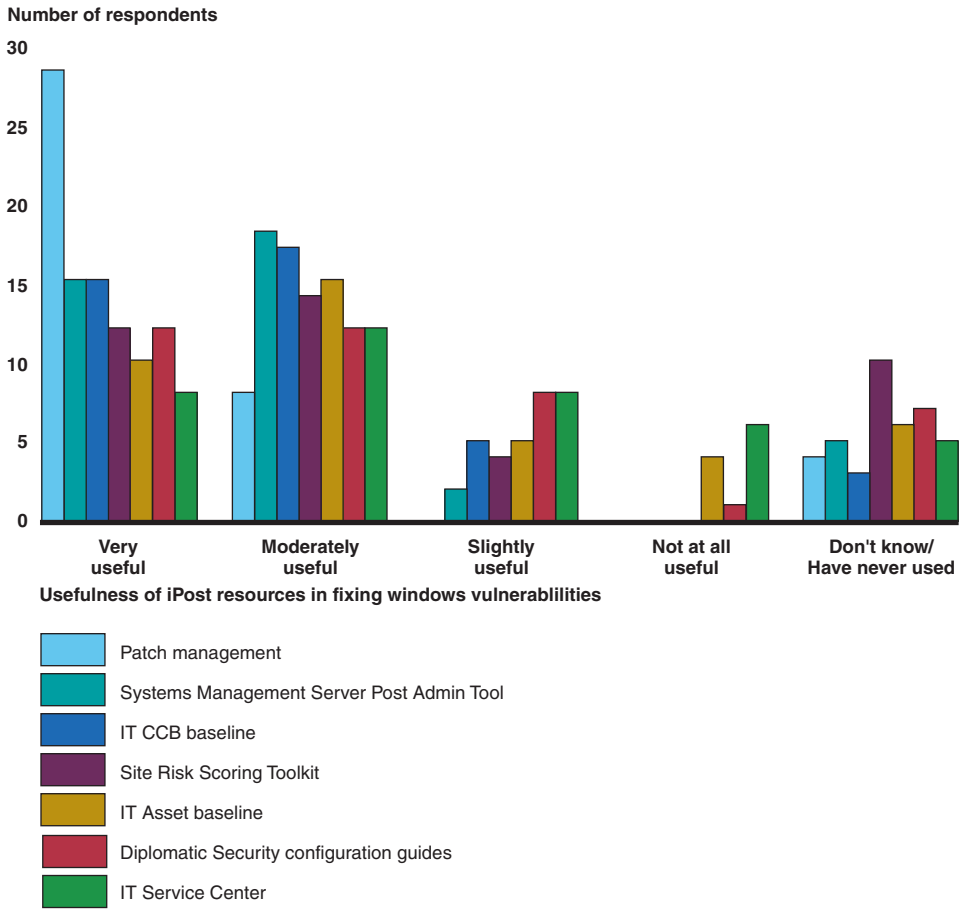
Table 4: Resource Links Available to Users in iPost

Resource	Description
Patch management Web site	Facilitates the management, installation, and monitoring of Windows operating system patches
SMS post admin tool	Allows an SMS Administrator to accomplish tasks required to administer an SMS system.
IT Change Control Board baseline	Includes a list of approved hardware and software that can be used on department systems that has been approved by the IT Change Control Board, which manages and approves changes to the department's IT infrastructure
Site Risk Scoring Toolkit	Provides online reference documents that iPost users can utilize for evaluating the site risk data and scores located in iPost
IT Asset baseline	Maintains the department's IT asset inventory
Diplomatic Security configuration guides	Documents the required configuration settings that should be in place for various operating systems
IT Service Center	Provides technical support for department users on IT-related issues

Source: GAO analysis of State documents.

State officials reported they used available resources linked in iPost to help them fix vulnerabilities at their sites and confirm those fixes were successfully implemented. In particular, the majority of survey respondents reported that the patch management Web site, the SMS post admin tool, and the IT Change Control Board baseline were very or moderately useful in helping them to fix vulnerabilities at their site. Over half of the 40 respondents stated that the Site Risk Scoring Toolkit (26), IT Asset baseline (25), and the Diplomatic Security configuration guides (24) were very or moderately useful in helping them to fix vulnerabilities at their site. However, officials also reported they had never used some of the resources available in iPost (see fig. 4).

Figure 4: Usefulness of iPost Resources in Fixing Windows Vulnerabilities



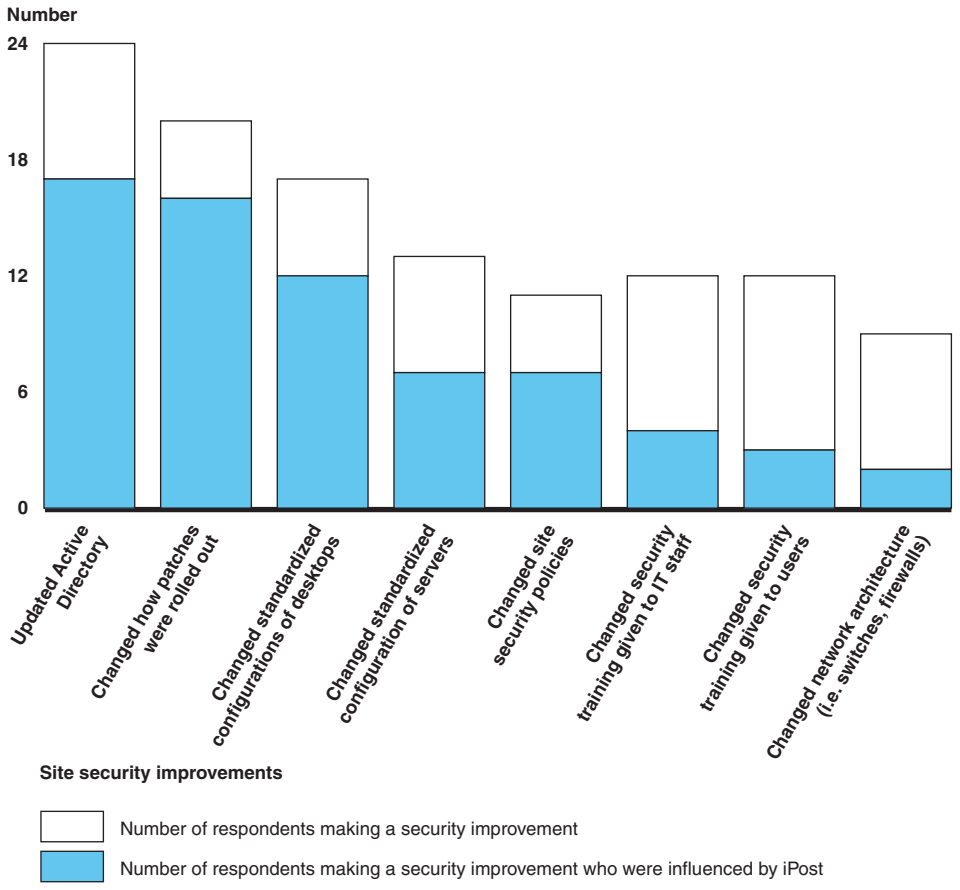
Source: GAO survey of State officials.

In addition, State officials mentioned they utilized iPost to confirm that fixes they made to identified vulnerabilities were successfully implemented. In particular, survey respondents reported they either waited for the next automated scan results to be posted in iPost (28 of 31 respondents) or e-mailed headquarters in Washington, D.C., to run another scan to see that the fix was implemented (9 of 31 respondents). Regarding the helpfulness of iPost in verifying vulnerability fixes were successfully implemented, survey respondents found iPost to be very helpful (17 respondents), moderately helpful (12 respondents), slightly helpful (5 respondents) or not at all helpful (2 respondents).

Using iPost Influenced Officials to Implement Other Security Improvements at Their Sites

State officials surveyed reported that using iPost also influenced them to make other security improvements at their sites. For example, of the 24 respondents who reported updating AD at their site, 17 respondents reported they were influenced by using iPost to do so, and of the 20 respondents that reported changing how patches were rolled out, 16 reported that iPost influenced them in making this change. In addition, several respondents reported making security improvements in configurations of servers, site security policies, security training, and network architecture based in part on their use of iPost (see fig. 5).

Figure 5: Site Security Improvements Influenced by Using iPost



Source: GAO survey of State officials.

For example, one survey respondent reported that since the desktops shipped to the site had obsolete software on the standardized baseline image, he/she removed the old software before deploying the workstations at the site. Another survey respondent reported that he/she looked at iPost to see whether deployed patches needed to be pushed out again or if they needed to be installed manually.

State Officials Did Not Incorporate iPost Results to Update Key Security Documents

NIST SP 800-37 states that continuous monitoring results should be considered with respect to necessary updates to an organization's security plan, security assessment report, and plan of action and milestones, since these documents are used to guide future risk management activities. The information provided by these updates helps to raise awareness of the current security state of the information system and supports the process of ongoing authorization and near real-time risk management.

However, State did not incorporate the results of iPost continuous risk monitoring activities into the OpenNet security plan, security assessment report, and plan of action and milestones on an ongoing basis. For example, plans of action and milestones were not created or updated for guiding and monitoring the remediation of vulnerabilities deemed to be exceptions.[19] Thus, key information needed for tracking and resolving exceptions was not readily available. As a result, the department may limit the effectiveness of those documents in guiding future risk management activities.

[19]An exception is created when a security weakness or vulnerability cannot be resolved by local administrators for technical or organizational reasons beyond local control. The score for the identified vulnerability is transferred to the organization responsible for addressing the exception.

State Has Implemented Controls Aimed at Ensuring the Timeliness, Accuracy, and Completeness of Data in iPost, but Opportunities for Improvement Exist

Organizations establish controls to provide reasonable assurance that their data are timely, free from significant error, reliable, and complete for their intended use. According to *Standards for Internal Control in the Federal Government,*[20] agencies should employ a variety of control activities suited for information systems to ensure the accuracy and completeness of data contained in the system and that the data is available on a timely basis to allow effective monitoring of events and activities, and to allow prompt reaction. These controls can include validating data; reviewing and reconciling output to identify erroneous data; and reporting, investigating, and correcting erroneous data. These controls should be clearly documented and evaluated to ensure they are functioning properly. NIST SP 800-39 also states that the processes, procedures, and mechanisms used to support monitoring activities should be validated, updated, and monitored. According to the Foreign Affairs Manual, stakeholders, system owners, and data stewards must ensure the availability, completeness, and quality of department data.

State has developed and implemented several controls that are intended to ensure the timeliness, accuracy, and completeness of iPost data. For example, State has employed the use of automated tools to collect monitoring data that are integrated into iPost. The use of automated tools is generally faster, more efficient, and more cost-effective than manual collection techniques. Automated monitoring is also less prone to human error. State also has used data collection schedules that support the frequent collection of monitoring data. For example, every Windows host at each iPost site is to be scanned for vulnerabilities every 7 days. The frequent collection of data helps to ensure its timeliness. In addition, State has established three scoring components—SMS Reporting, Vulnerability Reporting, and Security Compliance Reporting—in its risk scoring program to address instances when data collection tools do not correctly report the data required to compute a score for a component, such as when a host is not scanned. To illustrate, a host is assigned a score for the Vulnerability Reporting component if it misses two or more consecutive vulnerability scans (that is, the host is not scanned in 15 days). Intended to measure the risk of the unknown according to iPost

[20]GAO, *Standards for Internal Control in the Federal Government,* GAO/AIMD-00.21.3.1 (Washington, D.C.: November 1999). GAO also issued a management evaluation tool to assist agencies in maintaining or implementing effective internal control. See GAO, *Internal Control Management and Evaluation Tool,* GAO-01-1008G (Washington, D.C.: August 2001).

documentation, this scoring method also serves as a control mechanism for identifying and monitoring hosts from which data were not collected in accordance with departmental criteria.

State officials also advised that they had conducted a pilot program for the risk scoring program that enabled site users to (1) review the results of the data collections and associated scoring of the weaknesses and (2) report any inaccuracies they observed. State then identified solutions for the inaccuracies observed. Although the pilot was completed in April 2009, State officials noted they continue to rely on iPost users to report missed scans and inaccurate or incomplete data observed.

Notwithstanding these controls, the timeliness, accuracy, and completeness of iPost data were not always assured. For example, several instances where iPost data were not updated as frequently as scheduled, inconsistent, or incomplete are illustrated below.

- *Frequency of updates to iPost data supports federal requirements but vulnerability scanning was not conducted as frequently as State scheduled.* FISMA requires that agencies conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency based on risk but no less frequent than annually. According to iPost documentation, each host is to be scanned for vulnerabilities every 7 days. However, a review of scanning data for 15 sites (or 120 weekly scans) during an 8-week period in summer 2010 revealed that only 7 percent of the weekly scans successfully checked all Windows hosts at the site scanned. While 54 percent of the weekly scans successfully checked between 80 percent to 99 percent of the site's Windows hosts, 28 percent of the scans checked less than 40 percent of a site's hosts. Ten sites experienced at least one weekly scan cycle during which none of their hosts were scanned for vulnerabilities and a rescheduled scan was also not performed. According to iPost documentation, a host may not have been scanned because the host was powered off when the scan was attempted, the host's Internet protocol address was not included in the range of the scan, or the scanning tool did not have sufficient permissions to scan the host. Although the frequency of updates to iPost data supports State's efforts to satisfy FISMA's requirement for periodic testing and evaluation, the updates to vulnerability information in iPost were not as timely as intended. As a result, iPost users may base risk management decisions on incomplete data.

- *Data from vulnerability scans were sometimes not uploaded to iPost in a timely manner.* State officials stated that vulnerability scanning results are typically presented in the iPost staging database at least 1 day following the scan. However, the length of time it took for scan results to be uploaded into iPost was not consistent across all sites and impacted the scoring results for certain sites. The scanning results for the majority of 15 sites reviewed were typically presented in iPost at least 1 day following the scan, although it took up to 3 days for certain foreign and domestic sites. According to State officials, delays with uploading information to iPost for certain geographical areas around the world occurred because of the network's architecture. As a result, numerous Windows hosts at 6 of the 15 sites reviewed received scores in iPost's vulnerability reporting component for missing two consecutive vulnerability scans even though the hosts had been scanned. Consequently, iPost users may make risk management decisions based on inaccurate or incomplete data.
- *Data presented in iPost about the number of hosts addressed were sometimes inconsistent*. According to State officials, the information in iPost-generated reports should reflect the information displayed on iPost screens; however, information presented about the number of hosts was sometimes inconsistent. For example, the number of hosts that were not scanned for security compliance differed between the iPost reports and the site summary screens for each of the 15 sites reviewed. According to a State official, the summary screen displayed number of hosts that were not scanned over two weekly cycles whereas the iPost reports presented the number of hosts that were not scanned during the current weekly cycle but iPost did not clearly label the data elements accordingly. In addition, several iPost reports generated on the same day at one site showed a different number of hosts for which SMS did not report data. iPost-generated enterprise reports also varied in terms of the total number of hosts being monitored and scored, ranging from approximately 84,000 to 121,000. As a result, iPost users may base risk management decisions on inconsistent or inaccurate data.

Several factors contributed to the conditions described above. Technical limitations of the data collection tools contributed to missed scans. For example, the diagnostic scanning tool used by State performed agentless network scans of specific Internet protocol address ranges, so hosts that are powered off during the scan or are not included in the address range during the scan are missed. State officials were aware of the limitations with the scanning tool and indicated they had taken steps to address them. Specifically, State acquired and was implementing a new

diagnostic tool based on agent technology to collect vulnerability and security compliance data. Also, iPost did not retain detailed data from multiple cycles of scans of hosts at a site over an extended period since the data was overwritten by new scan results or was deleted. As a result, iPost users could not conduct trend analyses to determine the extent to which scans were successfully completed as scheduled or that data are accurately and consistently presented in iPost screens and reports. State recognized the importance of having detailed historical scan data. As noted earlier, a State official stated that a new policy was being implemented that requires detailed data be retained for two to three scans so that users at a site can see what changed.

In addition, State had not adequately documented all of the controls in place for ensuring the timeliness, accuracy, and completeness of data and based on our review, we could not determine if all of the stated controls were in place or working as intended. Further, State had not implemented formal procedures for systematically validating data and reviewing and reconciling output in iPost on an ongoing basis to detect and correct inconsistent and incomplete data, which State officials confirmed were not in place. Developing, documenting, and implementing these procedures and controls, and ensuring that they are working as intended, can provide increased assurance that information displayed in iPost is consistent, accurate, and complete.

iPost Provides Many Benefits, but Also Poses Challenges

State's implementation of iPost has resulted in improvements to the department's information security by providing extensive and timely information on vulnerabilities and weaknesses on Windows servers and workstations, 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 in implementing iPost. These challenges include overcoming limitations and technical issues with data collection tools, identifying and notifying individuals with responsibility for site-level security, implementing configuration management, and adopting a continuous monitoring strategy for moving forward in incorporating additional functionality into iPost.

Implementing iPost Has Helped State to Rapidly Identify and Fix Vulnerabilities on Windows Hosts

The implementation of iPost has enhanced information security at the department by offering a custom application with a common methodology for data collection, analysis, and reporting of information that security officers and system administrators can use to find extensive information on the security of Windows hosts that they are responsible for and fix specified vulnerabilities. For example, information in iPost allows users to:

- obtain a quick visual overview of compliance, vulnerability, patch, antivirus, and other component status for Windows hosts via the site summary report;
- access information about the status of security controls to determine the extent to which the controls are implemented correctly; and
- determine which hosts were scanned or not scanned and when this occurred.

iPost and the risk scoring program have also facilitated the identification of other potential security problems since users could make connections between pieces of data to find possible trends or patterns. For example, one official responded in the survey that he was able to identify a network performance problem by reviewing data available on the iPost portal and as a result, increase the data transmission rates over the network for his site. In addition, since regional and enterprise managers have access to iPost data for sites for the region or enterprise, they have increased awareness of security issues at specific sites and across the enterprise, allowing department officials a common language with which to discuss vulnerabilities and make decisions regarding their mitigation.

Moreover, the inclusion of a scoring approach, with associated ranking of sites and letter grades within iPost, has created a mechanism for the department chief information security officer to use in conveying to system administrators the department's priorities in addressing the mitigation of identified vulnerabilities or implementation of particular patches, among other things. The scoring method has motivated security officers and system administrators to focus on the vulnerabilities that have been given the highest scores first and mitigate these weaknesses on affected machines. This approach also allows regional and enterprise officials who review the letter grades and rankings to identify sites where improvements need to be made. Having this capability has enabled the department to respond to emerging threats associated with vulnerabilities in commercial products that occurred over the past year.

iPost implementation has also enhanced information security at State because having a continuous monitoring program in place provides

information on weaknesses affecting Windows devices. In particular, controls on these devices are assessed more often than the testing and evaluations of controls that are performed as part of certification and accreditation of OpenNet every 3 years. By taking steps to implement continuous monitoring through iPost, State has been able to obtain information on vulnerabilities and weaknesses affecting tens of thousands of Windows devices on its OpenNet network every couple of days, weekly, or biweekly. Having this type of capability has enabled department officials to identify vulnerabilities and fix them more rapidly than in years prior to iPost implementation.

Challenges Exist for State in Implementing Continuous Monitoring with iPost

Limitations in the capabilities of commercially available tools and technical issues with the tools used to collect data on vulnerabilities created challenges for State implementing a continuous monitoring program. State officials stated that when they initially began to conceptualize the application there were no commercial products available with the functionality and capabilities needed, so they developed iPost with the assistance of contractors. There were challenges involved with iPost's development, including resolving the technical issues with using scanning tools and displaying the results obtained from various data collection tools that had different data file formats. For example, State officials identified the following technical issues with the data collection tools:

- Certain tools did not always check each control setting as expected, did not always scan hosts when scheduled, or created false positives that had to be analyzed and explained.
- A vendor did not consistently keep its scanning tool up to date with the common vulnerabilities and exposures from the National Vulnerability Database.
- Scanning tools of different vendors used different approaches for scoring groups of vulnerabilities, so when the agent software scanner of a new vendor was implemented, State had to curve scores so that the disparities did not penalize the site.

Another challenge with running scans is that scanning tools do not have the capability to scan tens of thousands of hosts at one time without significant network performance degradation. Therefore, the department has had to establish scanning schedules so all hosts can be scanned over a period of time.

State officials stated they had taken steps to address these challenges by working with a vendor to enhance its data collection tool and selecting an alternate tool when appropriate. In addition, department officials stated they were working with other agencies and a contractor to develop additional capabilities that better meet their needs. Building these relationships could benefit the department as it moves forward in monitoring additional controls and developing additional capabilities in iPost.

Identifying and Notifying Individuals with Responsibility for Site-Level Security

According to *Standards for Internal Control in the Federal Government*,[21] authority and responsibility should be clearly assigned throughout the organization and clearly communicated to all employees. Responsibility for decision making is clearly linked to the assignment of authority, and individuals are held accountable accordingly.

iPost generally identified the local administrator(s) for each Windows host who would generally have the access permissions necessary to resolve nonexception weaknesses on the host. However, iPost did not identify the individual or contact point at each site or operational unit who had site-level responsibility for reviewing iPost site reports, monitoring the security state of the site's hosts, and ensuring that the control weaknesses identified on all hosts at the site were resolved. In particular, there was confusion at the department as to who was responsible for operational units when this information was requested, and the information that was subsequently provided was inaccurate for several units. As a result, the department has reduced assurance that responsibility for monitoring the security state of and resolving known weaknesses on a site's Windows hosts is clearly conveyed.

In addition, departmental officials did not always notify senior managers at sites with low security grades of the need to fix security weaknesses. According to State officials, operational units in iPost with grades C- or below for 3 consecutive months are to receive warning letters indicating the need to improve their grades.[22] From April 2009 to March 2010, 62 out of 483 sites received letters noting the need for improvement; however, 6 additional sites should have received letters but did not. In addition, 33

[21]GAO/AIMD-00-21.3.1; GAO-01-1008G.

[22]This information is maintained in a separate database outside of iPost to store historical information on site letter grades and the average host score in order to track the performance of sites over time.

sites that received at least one warning letter should have received one or more additional warnings for months with low grades but did not. As a result, senior managers may not have been fully aware of the security state of Windows hosts at sites they oversee.

Implementing Configuration Management for iPost

According to the Foreign Affairs Handbook, the development of new IT services, systems and applications, and feature and maintenance enhancements are to follow the guidance outlined in the Foreign Affairs Manual. The Foreign Affairs Manual states that configuration management[23] plans should be developed for IT projects and identify the system configuration, components, and the change control processes to be put in place. Effective configuration management also includes a disciplined process for testing configuration changes and approving modifications, including the development of test plan standards and documentation and approval of test plans, to make sure the program operates as intended and no unauthorized changes are introduced.

State had not fully implemented configuration management for iPost. Although the department had maintained release notes on updates, scoring documents, and presentations on iPost, key information about the program and its capabilities was not fully documented. For example, there were no diagrams of the architecture of iPost or a configuration baseline. In addition, there was no documentation of appropriate authorization and approval of changes included in iPost updates. Furthermore, although State improved its process for testing applications and subsequent versions of iPost from a manual and informal testing process in April 2010, it still lacks a written test plan and acceptance testing process with new releases being approved prior to release. For example, test procedures were not performed or documented to ensure that scripts for applying scoring rules matched the stated scoring methodology and that the scoring scripts were sufficiently tested to ensure that they fulfilled State's intended use.

As the department moves forward with implementation of additional capabilities for iPost, the need for a robust configuration management and testing process increases. Until such a process is fully developed,

[23]Configuration management allows an organization to develop requirements and implement appropriate controls to ensure requirements are met. Such controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely as intended.

documented, and maintained, State has reduced assurance that iPost is configured properly and updates or changes to the application and scoring rules are working as intended.

Adopting a Strategy for Continuous Monitoring of Controls

According to NIST, as part of a risk management framework for federal information systems, a strategy for the selection of appropriate security controls to monitor and the frequency of monitoring should be developed by the information system owner and approved by the authorizing official and senior information security officer. Priority for selection of controls to monitor should be given to controls that are likely to change over time. In addition, the security status of the system should be reported to the authorizing official and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy. The authorizing official should also review the effectiveness of deployed controls on an ongoing basis to determine the current risk to organizational operations and assets. According to the Foreign Affairs Manual, risk management personnel should balance the tangible and intangible cost to the department of applying security safeguards against the value of the information and the associated information system.

While State has reported success with implementing iPost to provide ongoing monitoring of certain controls over Windows hosts on OpenNet and reporting the status of these controls across the enterprise to appropriate officials, the department faces an ongoing challenge in continuing this success because it does not have a documented continuous monitoring strategy in place. Although the department began continuous monitoring before applicable detailed federal guidance was available and selected controls to monitor based on the capabilities of existing data collection tools, the department has not re-evaluated the controls monitored to determine whether the associated risk has changed. In addition, although department officials reported they were working to implement additional controls, there was no documentation to indicate whether the department had weighed the associated risk and the tangible and intangible costs associated with implementation when selecting which controls they intended to monitor. Furthermore, the frequency of how often the security status of the Windows hosts should be reported to the authorizing official and other appropriate officials was not documented. Therefore, until the department develops, documents, and implements a continuous monitoring strategy, the department may not have sufficient assurance that it is effectively monitoring the deployed security controls and reporting the security status to designated officials with sufficient frequency.

Managing Stakeholder Expectations for Continuous Monitoring Activities

Leading practices for program management, established by the Project Management Institute in *The Standard for Program Management,*[24] state that the information that program stakeholders need should be made available in a timely manner throughout the life cycle of a program. In addition, *Standards for Internal Control in the Federal Government*[25] states that information should be communicated to management and others within the agency who need it. Management should also ensure there are adequate means of communicating with external stakeholders that may have a significant impact on the agency achieving its goals. A further ongoing challenge for the department is understanding and managing internal and external stakeholders' expectations for continuous monitoring activities in terms of what goals and objectives can reasonably be achieved with iPost. These expectations include:

- *Lowering scores in iPost always implies that risks to the individual sites are decreasing.* With the current scoring approach used in iPost, lowering a score may imply that the associated risks to the site are being lowered as well, but there may be other reasons for the score being adjusted that are not related to mitigating the risk to particular hosts or sites. In particular, State officials have reported that (1) curving of the scores is performed in order to promote fairness; (2) exceptions are granted which shift the score from one operational unit to another; and (3) moving responsibility for hosts at overseas units to domestic units, which adjusts the scores accordingly. State officials should be careful in conveying to managers who make decisions based on scores and grades that lowering of scores in iPost doesn't necessarily indicate that risks to the department are decreasing.
- *Having continuous monitoring may replace the need for other assessment and authorization activities*. According to NIST, a well designed and managed continuous monitoring program can transform an otherwise static and occasional security control assessment and risk determination process that is part of periodic assessment and authorization into a dynamic process that provides essential, near, real-term security status-related information. However, continuous monitoring does not replace the explicit review and acceptance of risk

[24]Project Management Institute, *The Standard for Program Management*, *Second Edition* (Newton Square, Pa.: 2008).

[25]GAO/AIMD-00-21.3.1.

by an authorizing official on an ongoing basis as part of security authorization and in itself, does not provide a comprehensive, enterprisewide risk management approach. In addition, since continuous monitoring may identify risks associated with control weaknesses on a frequent basis, there may be instances where the problem cannot be fixed immediately, such as cases where State granted exceptions for weaknesses for periods of a year or more. There will need to be a mechanism in place for the designated authority to approve the associated risks from granting these exceptions. As the department moves forward with implementation of additional capabilities, it will be important to recognize the limitations of continuous monitoring when undertaking these efforts.

State officials confirmed that managing stakeholder expectations, in particular external stakeholders, had been a challenge. The Chief Information Security Officer (CISO) stated that the department was attempting to address these expectations by clarifying information or giving presentations to external audiences, and specifically communicated that iPost was not intended to entirely replace all certification and accreditation activities. If State continues to provide reliable and accurate information regarding continuous monitoring capabilities to both internal and external stakeholders, then the department should be able to effectively manage stakeholder expectations.

Conclusions

State's implementation of iPost has improved visibility over information security at the department by providing enhanced monitoring of Windows hosts on the OpenNet network with nearer-to-real-time awareness of security vulnerabilities. As part of this effort, State's development of a risk scoring program has led the way in creating a mechanism that prioritizes the work of system administrators to mitigate vulnerabilities; however, it does not incorporate all aspects of risk. Establishing a process for defining and prioritizing risk through a scoring mechanism is not simple and solutions to these issues have not yet been developed at State. Neverthless, State's efforts to work on addressing these issues could continue to break new ground in improving the visibility over the state of information security at the department.

iPost has helped IT administrators identify, monitor, and mitigate information security weaknesses on Windows hosts. In addition, State officials reported that using iPost had led them to make other security improvements at their sites. However, while iPost provides a useful tool

for identifying, monitoring, and reporting on vulnerabilities and weaknesses, State officials have not used iPost results to update key security documents which can limit the effectiveness of those documents in guiding future risk management activities.

As part of iPost implementation, State has implemented several controls that are intended to help ensure timeliness, accuracy, and completeness of iPost data; however, vulnerability scans were not always conducted according to State's schedule, and scanning results were uploaded to iPost in an inconsistent manner. Further, iPost data were not always consistent and complete. The acquisition and implementation of new data collection tools may help State overcome technical limitations of its scanning tool. Establishing robust procedures for validating data and reviewing and reconciling output on an ongoing basis to ensure data consistency, accuracy, and completeness can provide additional assurance to iPost users and managers who make risk management decisions regarding the allocation and prioritization of resources for security mitigation efforts at sites or across the enterprise based on iPost data.

iPost provides several benefits in terms of providing more extensive and timely information on vulnerabilities, while also creating an environment where officials are motivated to fix vulnerabilities based on department priorities. Nevertheless, State faces ongoing challenges with continued implementation of iPost. As State implements additional capabilities and functionality in iPost, the need increases for the department to identify and notify individuals responsible for site-level security, develop configuration management and testing documentation, develop a continuous monitoring strategy, and manage and understand internal and external stakeholder expectations in order to ensure the continued success of the initiative for enhancing department information security.

Recommendations for Executive Action

To improve implementation of iPost at State, we recommend that the Secretary of State direct the Chief Information Officer to take the following seven actions:

- Incorporate the results of iPost's monitoring of controls into key security documents such as the OpenNet security plan, security assessment report, and plan of action and milestones.
- Document existing controls intended to ensure the timeliness, accuracy, and completeness of iPost data.

- Develop, document, and implement procedures for validating data and reviewing and reconciling output in iPost to ensure data consistency, accuracy, and completeness.
- Clearly identify in iPost individuals with site-level responsibility for monitoring the security state and ensuring the resolution of security weaknesses of Windows hosts.
- Implement procedures to consistently notify senior managers at sites with low security grades of the need for corrective actions, in accordance with department criteria.
- Develop, document, and maintain an iPost configuration management and test process.
- Develop, document, and implement a continuous monitoring strategy that addresses risk, to include changing threats, vulnerabilities, technologies, and missions/business processes.

Agency Comments and Our Evaluation

In written comments on a draft of this report signed by the Chief Financial Officer for the Department of State, reproduced in appendix III, the department said the report was generally helpful in identifying the challenges State faces in implementing a continuous monitoring program around the world. In addition, State described metrics that it uses for correcting known vulnerabilities and measuring relative risks at sites. The department also concurred with two of our recommendations, partially concurred with two, and did not concur with three.

Specifically, State concurred with our recommendations and indicated that it has or will (1) implement procedures to consistently notify senior managers at sites with low security grades of the need for corrective actions, in accordance with department criteria, and (2) develop, document, and implement a continuous monitoring strategy.

State partially concurred with our recommendation to develop, document, and implement procedures for validating data and reviewing and reconciling output in iPost to ensure data consistency, accuracy, and completeness. The department stated that it had developed and implemented procedures for validating and testing output in iPost by scanning for vulnerabilities every 7 days and establishing three scoring components to score hosts when data collection tools do not correctly report the data required to compute a score. We agree and acknowledge in our report that the department has established these controls; however, the controls do not always ensure that if data is collected, it is accurate

and complete. As mentioned in the report, we identified instances where iPost data was inconsistent, incomplete, or inaccurate, including the scoring of hosts for missed vulnerability scans when a scan had occurred. State officials make decisions about the prioritization of control weakness mitigation activities and allocation of resources based on information in iPost and so the accuracy and completeness of that information is important. Having procedures for validating data and reconciling the output in iPost will help ensure that incomplete or incorrect data is detected and corrected, and documenting these procedures will help ensure that they are consistently implemented.

State also partially concurred with our recommendation that the department develop, document, and maintain an iPost configuration management and test process. The department questioned the need to have a diagram of the architecture of iPost and a written test plan and acceptance testing process, and stated that our report noted State had improved its process for testing versions of iPost. We have modified the report to provide additional context for the statement regarding State's testing process in order to clarify any misunderstanding. In addition, as mentioned in the report, we identified areas where testing procedures were not performed or documented, including ensuring the scripts for applying the scoring rules matched the stated scoring methodology. In addition to lacking basic diagrams showing iPost interactions, we also determined that the department lacked a configuration baseline and documented approval process for iPost changes. Having a robust configuration management and testing process helps to provide reasonable assurance that iPost is configured properly, that updates or changes to the application are working as intended, and that no authorized changes are introduced, all of which helps to ensure the security and effectiveness of the continuous monitoring application.

State did not concur with our recommendation for incorporating the results of iPost's monitoring of controls into key security documents such as the OpenNet security plan, security assessment report, and plan of action and milestones. State did not provide a rationale for its nonconcurrence with our recommendation, and instead focused on providing additional information about the department's use of metrics related to assigning risk values. As NIST guidance indicates, incorporating results from continuous monitoring activities into these key documents supports the process of ongoing authorization and near real-time risk management. In addition, as mentioned in the report, State has granted exceptions for weaknesses in iPost for periods of a year or more but has not created or updated plans of action and milestones to guide

and monitor the remediation of these exceptions. Continuous monitoring does not replace the explicit review and acceptance of risk by an authorizing official on an ongoing basis as part of security authorization. The results of iPost's monitoring of controls, including the ongoing monitoring and remediation of the exceptions, needs to be documented in order to identify the resources and timeframes necessary for correcting the weaknesses. In addition, the designated authority will need to review these results to ensure OpenNet is operating at an acceptable level of risk.

In addition, the department did not concur with our recommendation to document existing controls intended to ensure the timeliness, accuracy, and completeness of iPost data because it stated that it regularly evaluates iPost data in these areas and stated that further documentation was of questionable value. However, as mentioned in our report, we identified incomplete, inconsistent, or inaccurate data in iPost during our review and could not determine if all of the controls the department told us they implemented were actually in place or working as intended. Documenting the controls helps to provide assurance that all appropriate controls have been considered and can be used as a point of reference to periodically assess whether they are working as intended.

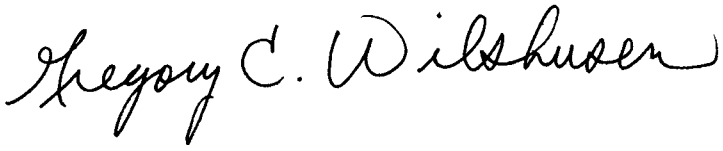
The department also did not concur with our recommendation to clearly identify in iPost individuals with site-level responsibility for monitoring the security state and ensuring the resolution of security weaknesses of Windows hosts. The department noted that it failed to understand the necessity for individually naming those staff with site-level responsibility in iPost since we had surveyed State officials regarding their use of iPost. As we noted in the report, the department relies on users to report when inaccurate and incomplete iPost data and scoring is identified, so that it may be investigated and corrected as appropriate—even though there is no list in iPost showing who is responsible for a particular operational unit. As we discovered when we surveyed State officials, there was confusion at the department as to who was responsible for operational units and information provided to us on who was responsible was incorrect for several units. To clarify this issue, we have incorporated additional context in the report on identifying individuals with responsibility for site-level security.

Lastly, the department did not concur with our findings that the iPost risk scoring program does not provide a complete view of the information security risks to the department. Although the department's response generally did not address the findings made in the report, the department

did state that progress in addressing control weaknesses in iPost had led to an 89 percent reduction in measured cyber security risk and that it was impossible and impracticable to cover all areas of information security and security controls in NIST 800-53 as part of a continuous monitoring program. However, we did not state that all areas of information security and all controls in NIST 800-53 should be monitored as part of such a program. Rather, we stated that because iPost monitors only Windows devices and not other devices on OpenNet, addresses a select set of controls, and because State officials could not demonstrate the extent to which all components that are needed to measure risk— threats, the potential impacts of the threats, and the likelihood of occurrence—were considered when developing the scoring, that iPost does not provide a complete view of the information security risks to the department. Furthermore, as we mentioned in the report, the department should exercise care in implying that the lowering of scores in iPost means that risks to individual sites are decreasing as there may be other reasons for the score being adjusted that are not related to the mitigation of risk to particular hosts or sites, such as curving of scores or shifting of scores from one operational unit to another. While such activities may promote fairness, the lowering of scores may not necessarily indicate that risks to the department are decreasing.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the Secretary of State and interested congressional committees. The report will also be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions regarding this report, please contact me at (202) 512-6244 or at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix IV.



Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to determine (1) the extent to which the Department of State (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 address our objectives, we conducted our review in Washington, D.C., where we obtained and analyzed program documentation, reports, and other artifacts specific to iPost, the scoring program and components, and data collections tools; and interviewed State officials. To address the first objective, we analyzed guidance from the National Institute of Standards and Technology (NIST) on risk management and vulnerability scoring and compared it to iPost risk scoring documentation to determine whether the department's criteria and methodology were consistent with federal guidance. Where documentation on the department's process for defining and prioritizing risk did not exist, we obtained information from agency officials in these areas where possible. We also interviewed agency officials from NIST to obtain information on the Common Vulnerability Scoring System and how agencies can use the scoring to more accurately reflect risk to agency environments.

To address the second objective, we conducted interviews with State's Chief Information Officer, Deputy Chief Information Officer for Operations, Chief Information Security Officer, selected Executive Directors, Regional Computer Security Officers, and Information Systems Officers or Information Systems Security Officers to obtain information on how these officials used iPost, in particular what information or summary reports they used from iPost to make decisions about security improvements and what types of security improvements were made. We analyzed the information provided by the officials to determine patterns regarding what information were used from iPost and what types of improvements were made.

For the third objective, we analyzed department requirements for frequency of updates, accuracy, and completeness of iPost data to determine what controls should be in place. We obtained documentation and artifacts on department controls, or other mechanisms or procedures for each of the scoring components covered in iPost related to frequency, accuracy, and completeness of data and compared these to department requirements. Where the department lacked requirements in these areas, we analyzed our guidance on internal controls and assessment of controls for data reliability to determine what criteria should be in place to

provide sufficient assurance of accurate, complete, and timely data. In areas where documentation on the department's controls did not exist, we obtained information from department officials where possible.

We also selected 15 units from the list of operational units to perform analyses to determine the frequency, accuracy, and completeness of data in iPost. Operational units were selected based on location (domestic or overseas), the number of hosts at the site, and bureau to ensure representation from among geographic and functional bureaus within the department. Frequency data obtained from iPost was tabulated to determine the number of hosts scanned and the dates scanned, and then the data was compared to the scanning schedule to determine the frequency in which scans occurred at the site for the time period of July 19, 2010, through September 8, 2010. For accuracy and completeness, we compared detailed screens on information related to vulnerability and security compliance components for each of the above 15 sites with generated reports obtained from iPost. We also obtained raw scan data from State's scanning tool for three financial center sites and compared that to iPost to check frequency and accuracy, however, an analysis of the data obtained determined it was unusable due to inconsistencies with how the data were reformatted when viewed. In addition, for completeness, we obtained detailed screen information on the configuration settings scanned as part of the security compliance component from one site and compared the scanned settings evaluated to the list of required settings in a Diplomatic Security mandatory security setting document for Windows XP.

To address the fourth objective, we analyzed federal guidance on what activities should be taken as part of implementation of continuous monitoring, as well as department policies and guidance related to information technology management and projects and compared it to department activities undertaken for iPost implementation. We also obtained descriptions of benefits and challenges from the Chief Information Officer, Deputy Chief Information Officer for Operations, Chief Information Security Officer, selected Executive Directors, Regional Computer Security Officers, and Information Systems Officer or Information Systems Security Officers. We analyzed the information obtained from the department, federal guidance, and the results of our findings for the other objectives to identify patterns related to the benefits and challenges of implementation.

For our second, third, and fourth objectives, we also obtained information through a survey of individuals at domestic and overseas sites to

understand iPost current capabilities as of August of 2010. We surveyed individuals at 73 of the 491 operational units in iPost. We selected survey sites by reviewing the list of operational units in iPost and chose domestic sites from among each of the functional bureaus, and overseas sites from among each of the geographic bureaus to make sure there was coverage for each bureau and region in the sample. Sites within each functional and geographic bureau were selected based on the number of hosts at the site and the current letter grade received in order to include sites with varying numbers of hosts and grade scores. We developed a survey instrument to gather information from domestic and overseas department officials on how they used iPost at their location, whether they had experienced problems with using data collection tools, and what benefits and challenges they had experienced with implementation between August 1, 2009, and August 30, 2010. Our final sample included 73 sites (36 overseas and 37 domestic). The sample of sites we surveyed was not a representative sample and the results from our survey cannot be generalized to apply to any other sites outside those sampled. However, the interviews and survey information provided illustrative examples of the perspectives of various individuals about iPost's current and future capabilities. We identified a specific respondent at each site by either reviewing the contact list on State's Web site or asking State officials. This person was the Information Management Officer, Information System Officer, System Administrator, or Information System Security Officer, or the acting or assistant official in one of these positions at a given site.

To minimize errors that might occur from respondents interpreting our questions differently from our intended purpose, we pretested the questionnaire by phone with State officials who were in positions similar to the respondents who would complete our actual survey during four separate sessions. During these pretests, we asked the officials to complete the questionnaire as we listened to the process. We then interviewed the respondents to check whether (1) the questions were clear and unambiguous, (2) the terms used were precise, (3) the questionnaire was unbiased, and (4) the questionnaire did not place an undue burden on the officials completing it. We also submitted the questionnaire for review by a GAO survey methodology expert. We modified the questions based on feedback from the pretests and review, as appropriate.

Overall, of the 73 sampled sites, 40 returned completed questionnaires and 2 of the nonresponding sites were ineligible because they had been consolidated into other sites, leading to a final response rate of 57.1

percent; however, not all respondents provided answers to every question. Two of the sites answered about their own site and other sites under their supervision; each of these was treated as a single data point (i.e., site) in statistical analyses. We reviewed all questionnaire responses, and followed up by phone and e-mail to clarify the responses as appropriate.

The practical difficulties of conducting any survey may introduce nonsampling errors. For example, differences in how a particular question is interpreted, the sources of information available to respondents, or the types of respondents who do not respond to a question can introduce errors into the survey results. We included steps in both the data collection and data analysis stages to minimize such nonsampling errors. We examined the survey results and performed computer analyses to identify inconsistencies and other indications of error, and addressed such issues as necessary. An independent analyst checked the accuracy of all computer analyses to minimize the likelihood of errors in data processing. In addition, GAO analysts answered respondent questions and resolved difficulties respondents had answering our questions. We analyzed responses to closed-ended questions by counting the response for all sites and for overseas and domestic sites separately. For questions that asked respondents to provide a narrative answer, we compiled the open answers in one document that was analyzed and used as examples in the report.

We conducted this performance audit from March 2010 to July 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

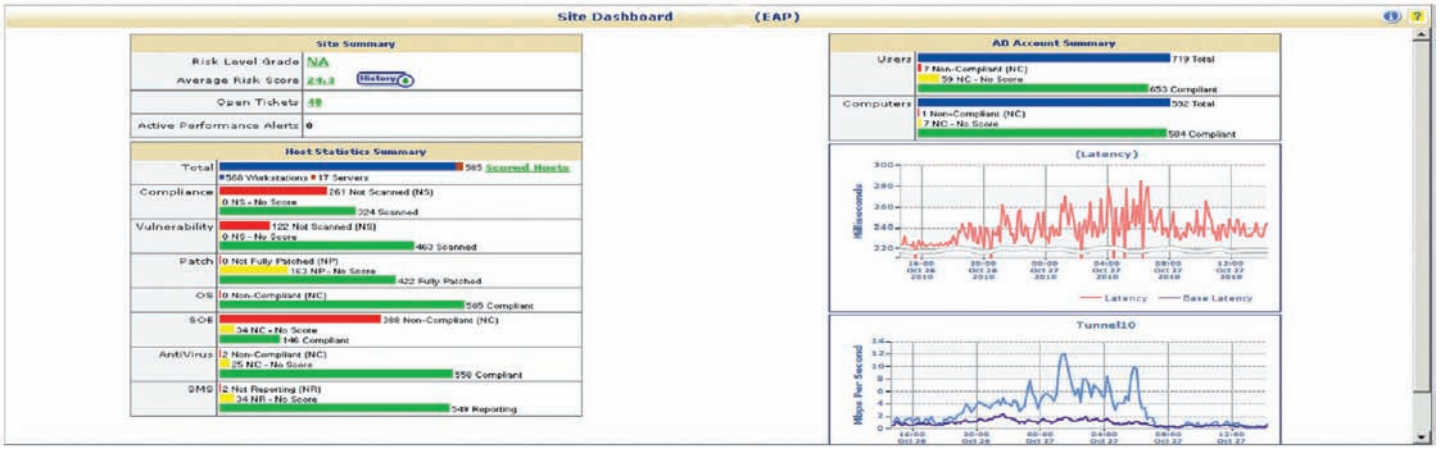
Appendix II: Examples of Key iPost Screens and Reports

A selection of key iPost screens and reports for sites are described below.

Site summary screen

The screen provides summary information on the site including: site's grade; host summary statistics by category which provides a graphical representation of the number of hosts that are compliant or not compliant; Active Directory (AD) account information for users and computers; and network activity at the site (see fig. 6).

Figure 6: Example of an iPost Dashboard Site Summary Screen

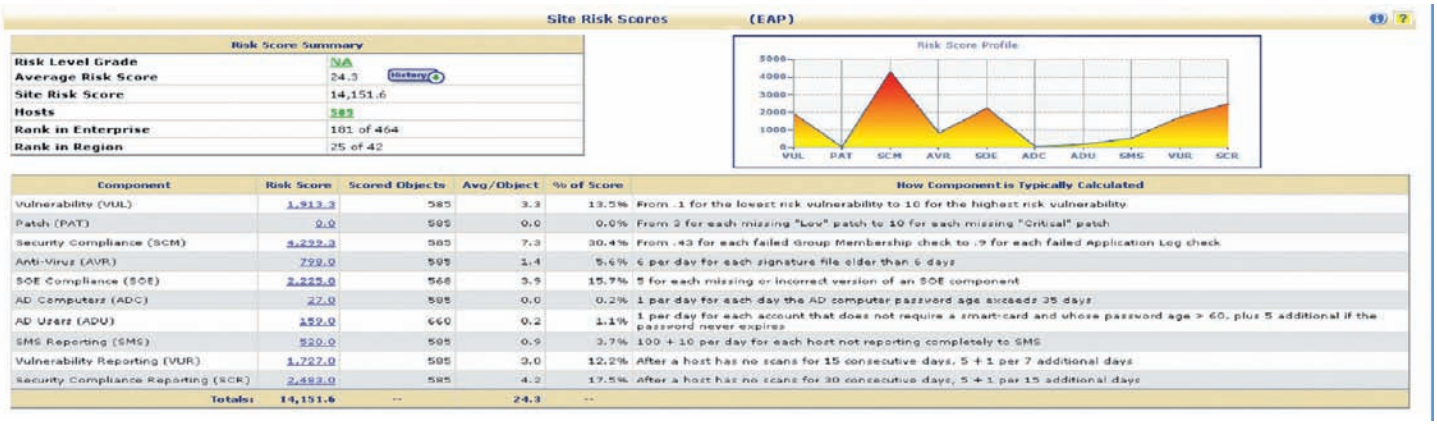


Source: State.

Site risk score summary screen

The site risk score summary screen provides a summary of the site's risk score summary, including the site's grade, average risk score, and total risk score. A summary table shows the total risk score broken down by category. A graphical presentation of the risk score by component highlights components with high risk scores (see fig. 7).

Figure 7: Example of an iPost Site Risk Score Summary Screen



Site Risk Scores (EAP)

Risk Score Summary

Risk Level Grade	NA
Average Risk Score	24.3 History
Site Risk Score	14,151.6
Hosts	585
Rank in Enterprise	181 of 464
Rank in Region	25 of 42

Risk Score Profile

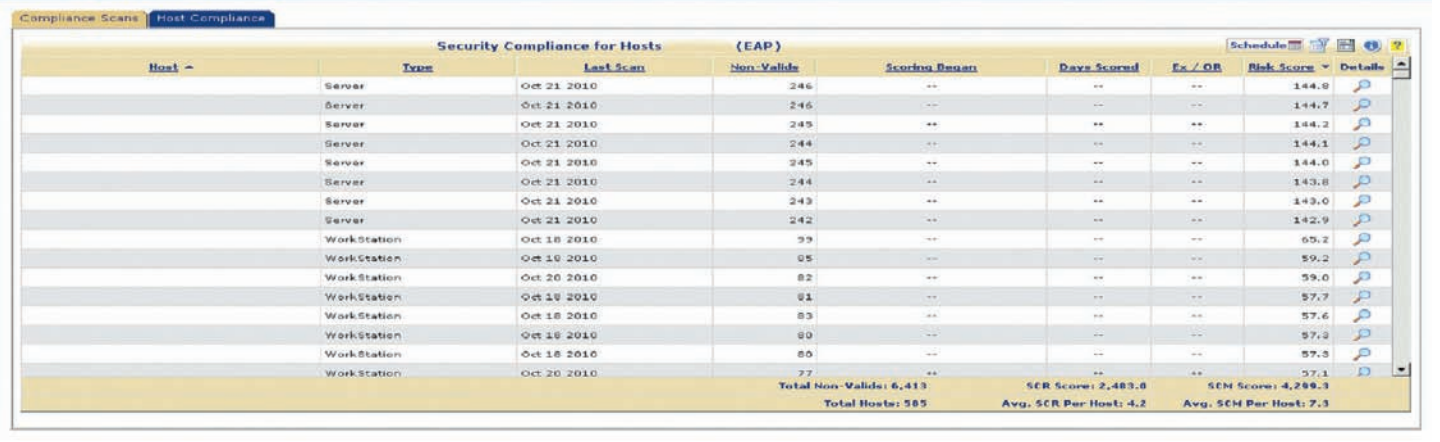
Component	Risk Score	Scored Objects	Avg/Object	% of Score	How Component is Typically Calculated
Vulnerability (VUL)	1,913.3	585	3.3	13.5%	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
Patch (PAT)	0.0	585	0.0	0.0%	From 2 for each missing "Low" patch to 10 for each missing "Critical" patch
Security Compliance (SCM)	4,293.3	585	7.3	30.4%	From .43 for each failed Group Membership check to .9 for each failed Application Log check
Anti-Virus (AVR)	799.0	585	1.4	5.6%	6 per day for each signature file older than 6 days
SOE Compliance (SOE)	2,225.0	568	3.9	15.7%	5 for each missing or incorrect version of an SOE component
AD Computers (ADC)	27.0	585	0.0	0.2%	1 per day for each day the AD computer password age exceeds 35 days
AD Users (ADU)	159.0	660	0.2	1.1%	1 per day for each account that does not require a smart-card and whose password age > 60, plus 5 additional if the password never expires
SMS Reporting (SMS)	520.0	585	0.9	3.7%	100 + 10 per day for each host not reporting completely to SMS
Vulnerability Reporting (VUR)	1,727.0	585	3.0	12.2%	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days
Security Compliance Reporting (SCR)	2,483.0	585	4.2	17.5%	After a host has no scans for 30 consecutive days, 5 + 1 per 15 additional days
Totals:	14,151.6	--	24.3	--	

Source: State.

Detailed component screens

Detailed component screens provide breakdowns of the scoring results for each host. For example, the detailed security compliance screen (see fig. 8) identifies each host, the type of host, the date of the last security compliance scan, and the total risk score assigned the host. Users can select the details option to see more specific information on the security settings that failed compliance and the associated score that was assigned.

Figure 8: Example of an iPost Detailed Security Compliance Component Screen



Compliance Scans | Host Compliance

Security Compliance for Hosts (EAP)

Schedule

Host	Type	Last Scan	Non-Valids	Scoring Began	Days Scored	Ex / OR	Risk Score	Details
	Server	Oct 21 2010	246	--	--	--	144.8	
	Server	Oct 21 2010	246	--	--	--	144.7	
	Server	Oct 21 2010	245	--	--	--	144.2	
	Server	Oct 21 2010	244	--	--	--	144.1	
	Server	Oct 21 2010	245	--	--	--	144.0	
	Server	Oct 21 2010	244	--	--	--	143.8	
	Server	Oct 21 2010	243	--	--	--	143.0	
	Server	Oct 21 2010	242	--	--	--	142.9	
	WorkStation	Oct 18 2010	99	--	--	--	65.2	
	WorkStation	Oct 19 2010	95	--	--	--	59.2	
	WorkStation	Oct 20 2010	82	--	--	--	59.0	
	WorkStation	Oct 19 2010	91	--	--	--	57.7	
	WorkStation	Oct 18 2010	83	--	--	--	57.6	
	WorkStation	Oct 19 2010	80	--	--	--	57.3	
	WorkStation	Oct 18 2010	80	--	--	--	57.3	
	WorkStation	Oct 20 2010	77	--	--	--	57.1	
			Total Non-Valids: 6,413		SCR Score: 2,483.0		SCM Score: 4,293.3	
			Total Hosts: 585		Avg. SCR Per Host: 4.2		Avg. SCM Per Host: 7.3	

Source: State.

Risk score advisory report

The risk score advisory report provides a summary of all the scoring issues for the site and summary advice on how to improve the site's score. Summary information includes the site's grade, average risk score, and total risk score. A graphical presentation of the risk score by component highlights components with high risk scores (see fig. 9).

Figure 9: Example of an iPost Risk Score Advisory Report

Source: State.

Appendix III: Comments from the Department of State

United States Department of State

Chief Financial Officer

Washington, D.C. 20520

JAN 28 2011

Ms. Jacquelyn Williams-Bridgers
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Ms. Williams-Bridgers:

We appreciate the opportunity to review your draft report, "INFORMATION SECURITY: State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain," GAO Job Code 311046.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact Jason Kerben, Senior Analyst, Bureau of Information Resource Management at (703)812-2378.

Sincerely,

James L. Millette

cc: GAO – Gregory C. Wilshusen
IRM – Susan H. Swart
State/OIG – Evelyn Klemstine

Department of State Comments on GAO Draft Report

INFORMATION SECURITY: State has Taken Steps to Implement a Continuous Monitoring Application, But Key Challenges Remain (GAO-11-149, GAO Code 311046)

The Department of State appreciates the opportunity to comment on the draft report, which we believe is generally helpful in identifying the challenges we face with implementing a continuous monitoring program around the world and in ensuring that the appropriate degree of security is applied in a risk management framework. Since the passage of the Federal Information Security Management Act (FISMA) of 2002, the nature of the threats posed to the federal government has increased exponentially. The Department has applied the highest amount of attention and focus to this ever-changing threat and will continue to do so. The Department employs a layered approach to security risk management by employing multiple levels of protection. This protection is accomplished by implementing a matrix of technical, operational, and management security controls designed to thwart network threats, detect and mitigate vulnerabilities, and strengthen business operations.

Cyber attack incidents recorded at the Department of State increased from 2,104 in calendar year 2008 to more than 3,000 in the first six months of 2010. Attacks were measured by the number of information security service tickets opened after incidents reported by 260 embassies, consulates, and 150 domestic organizations. During the same period, the proportion of attacks involving malicious software code grew from 39 percent to 84 percent. To find answers to these trends, the American computer security team supported foreign affairs network operations around the globe.

Accordingly, the Department applied policies and practices that are consistent with the principles espoused in an earlier GAO report on the subject of information security, in which GAO provided in the "Opportunities Exist for Enhancing Federal Cybersecurity" section of the report:

> In addition, agencies can also increase their efficiency in securing and monitoring networks by expanding their use of automated tools as part of their monitoring programs for performing certain security-related functions. For example, agencies can better use centrally administered automated diagnostic and analytical tools to continuously scan network traffic and

devices across the enterprise to identify vulnerabilities or anomalies from typical usage and monitor compliance with agency configuration requirements. GAO Report, "Information Security: Concerted Response Needed to Resolve Persistent Weaknesses," GAO 10-536T.

Today, as a result of the efforts discussed in the subject GAO report, a steady rotation of embassies, consulates, and passport production facilities send results of the electronic scans up to three times a day to a security data warehouse in the Eastern United States. Scanning tools have varied over time, but automatic scans of the software and operating systems on State Department personal computers and servers now occur every one to 15 days. By the end of 2010, the frequency of scans for vulnerabilities, configuration settings, password age, patching, and the viability of the scanning sensors themselves will occur every 24-72 hours. Other defensive cyber security scanning activities beyond personal computers and servers of the Department are headed in this direction of full automation.

As the scan results are sorted and recorded, a story is written in zeros and ones on the database tables of the security data warehouse. Once a day a new calculation is made that shows security teams at the Department of State their progress in correcting known vulnerabilities and other common cyber security problems. Point scores are in turn converted to letter grades of A+ to F- in ways the security managers may have last seen during their scholastic training. The story on cyber problems is different in each corner of the globe, and consequences of failing grades have never been more urgent.

Answering the call for actionable information to protect business continuity, the dashboard called iPost delivers customized snapshots of the worst cyber problems. From this data source, the immediate staff of Ambassadors, Assistant Secretaries, and their cyber security managers alike can learn which security factors, among 10, pose the greatest threats from computer attacks by hackers and adversaries. Armed for preventing the worst attacks they could face that day on their personal computers and servers, the security and system managers can fashion a tactical response to specific problems at their site.

Harnessing this mountain of metrics for correcting known vulnerabilities and re-calculating letter grades from A+ to F- for daily progress resulted in an initial 89 percent reduction in measured cyber security risk on personal computers and servers for each embassy, consulate, and headquarters organizations in the 12 months ending July 2009. In 2003, at the U.S. Agency for International

Development, two-thirds of measured risk on a broader range of system and network vulnerabilities was eliminated in six months.

The idea of "*information overload*" made popular by Alvin Toffler, suggests that people can have difficulty understanding issues and deciding what to do because of the "presence of too much information." Numerous studies have seized on the related problems that pilots face in war from reading unorganized cockpit instrumentation. For example, Mica R. Endsley and Robert P. Smith note the following in their article, "*Attention Distribution and Decision Making in Tactical Air Combat*":

> Even with the handicap of constrained information about the environment, there is a tremendous problem with information overload. Piecemeal addition of systems and lack of integration of information are often cited as major contributing factors.

To address the problem of information overload that plagues the foot soldiers in cyber conflict, the Department of State began experimenting with a range of solutions that could be adjusted for when, where, and how information on known security problems is delivered up for action. The Google – "Operation Aurora" attack, publicized in January 2010, is a good case study.

The Department of State, like the rest of the U.S. federal government, faced the arduous task of remediating two Internet Explorer vulnerabilities in succession to protect against exfiltration of data and account information. As part of the initial defensive response, a Microsoft Internet Explorer patch number MS10-012 needed to be installed on 94,200 workstations in 24 time zones without delay. To mobilize against this potential attack vector, the Department of State set aside the usual zero-to-10 risk-point scale and created a "special threat designation."

Patching progress on Operation Aurora follows a pattern of predictable behavior that our experts have been statistically tracking for over seven years. Risk points estimate the relative threat value of uncorrected cyber security problems. Points accumulate as measured by regular scanning and disappear from the risk accounts when the problems are corrected. Risk points have a universally accepted value across the 400 computer management organizations of the Department of State, but of course the number of devices, cyber problems, and associated risk point totals vary each location.

For the purposes of enterprise-level defensive cyber security, the Department needed to measure the relative risk per site. By adding the risk points measured by scans of their equipment and dividing by the total number of personal computers and servers, an embassy's average share of risk could be evaluated consistently in comparison with progress in the rest of the Department.

To analyze readiness against known attacks across the Department of State as an enterprise, the grade curve initially used an average of 40 risk points or less per host as the dividing line for grade of an A+ with a graduated scale of up to F. Grading on a curve began in July 2008, with an approximately equally number of A and F scores along with the expected larger number of Cs. This grade curve had a technical component, but the approach to business change is judged to be more instrumental to a favorable outcome over time.

At both USAID and the Department of State, it has proven essential to begin each pilot activity with an achievable outcome for some part of the community, no matter how low or unacceptable that initial grading standard was. Four No. 10 vulnerabilities on the Common Vulnerability Scoring Systems (CVSS) scale, or 40 points per host, is hardly laudable, but if everyone were rated D and F at the outset, the pattern of desired progress would never emerge. This approach of addressing the most critical vulnerabilities in a prioritized manner with a scaled score has been recognized as appropriate by both DHS and NSA.

When the participating managers see that success is achievable and begin to see part measurable improvements at their own sites, a contagious pattern of competition and continuous improvement begins to occur. This atmosphere functions like an engine fueled on a combination of metrics and professional competition. Yet, **confidence that the measurement system or market of risk is fair cannot be underestimated**.

As an example, on March 28, 2009, a 250-point drop in risk was reassigned to headquarters from embassies and consulates. This change marked the culmination of several months of discussion among overseas security managers. Security scanners determined that a headquarters-sponsored administrative software suite's version of Java Runtime Environment (JRE) was two generations out of date. A range of associated security problems were showing up in embassy risk score cards and letter-grade improvement on cyber security at embassies was stalled. Embassy security managers argued that they could not fix this corporate application. So, on that day, risk points discovered by scans for JRE problems were reassigned from embassies to the software development executive at corporate headquarters until

the software could be updated. This process of granting exceptions is limited to cases where a problem cannot be fixed at a particular site or when the scanners consistently and incorrectly record false positives for a particular deficiency. Managing exceptions takes time and detailed adjustments in the security dashboard, but the effort was judged essential to protect confidence and fairness in the execution of the risk market.

By late 2009, a disproportionately high percentage of the Department of State organizations rated a letter grade of A and B. To re-establish a normal curve of letter grade distribution, in early 2010 the coalition of organizations responsible for defensive cyber security at the Department began re-calibrating the grading scale in six equal increments to make it three times more difficult to achieve the same letter grade shown in yellow on the same diagram. By July 2010, only part way through the change toward tougher grading standards, the amount of measured risk on personal computers and servers had moved from at least 89 percent to 93 percent overall for the Department of State. This change represented an improvement of one-third of the remaining risk problems to correct, even after subtracting for security issues that could not be repaired by local system managers because of technical problems beyond their control.

When Congress began issuing letter grades to U.S. Cabinet Departments in 2002 under FISMA, the Department of State accumulated four Fs and one D- grade in the first five years. To improve, the Department needed to find a way to take the F grade off the shoulders of the top technical managers in Washington and push resolution of the cyber problems out to the far reaches of the organization. It was out of this urgency, to match accountability for problems that could only be fixed on the local level, that metrics materialized that would measure corrective action, a market of risk, and letter grades for tracking accountability for improvements in security.

We appreciate GAO's acknowledgement that "State has been the forefront of federal efforts in developing and implementing a continuous monitoring capability." However, the Department's efforts have been undertaken in an environment that is far from mature, as GAO has noted: "National Institute of Standards and Technology (NIST) *is in the process* of developing guidance that extends the Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) framework provided by DHS. NIST's extension is to provide information on an enterprise continuous monitoring technical reference architecture to enable organizations to aggregate collected data from security tools, analyze the data, perform scoring, enable queries, and provide overall situational

awareness." (Emphasis added.) GAO also notes that in the aforementioned DHS CAESARS framework, DHS "recognized State as a leading federal agency and noted that DHS's proposed target-state reference architecture for security posture monitoring and risk scoring is based, in part, on the work of State's security risk scoring program. In addition, in 2009, the National Security Agency presented an organizational achievement award to State's Site Risk Scoring program team for significantly contributing to the field of information security and the security of the Nation."

We note the draft GAO report provides that the "iPost risk scoring program helps to identify, monitor, and prioritize 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."

While achieving security of "all areas affecting information security," as GAO suggests is admirable, it is impossible and impracticable. OMB requires only *adequate security*, which is defined by OMB A-130 Appendix III as "security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." Furthermore, the very first sentence of NIST Special Publication 800-53 states that "the selection and implementation of *appropriate* security controls for an information system or a system of systems are important tasks that can have major implications on the operations and assets of an organization as well as the welfare of individuals and the Nation." (Emphasis added.) NIST's guidance provides that "it is the responsibility of organizations to select *appropriate* security controls, to implement the controls correctly, and to demonstrate the effectiveness of the controls in satisfying their stated security requirements" and that "organizations are expected to apply the supplemental guidance as *appropriate*, when defining, developing, and implementing security controls," but the guidance is silent with respect to how and to what degree those appropriate security controls should be prioritized in light of the unique threats and vulnerabilities facing that agency. (Emphasis added.)

Accordingly, the Department of State's continuous monitoring risk scoring program was established and implemented with the intent of achieving appropriate, prioritized security, tailored to the unique threats and vulnerabilities facing the Department.

Our responses to GAO's seven recommendations follow:

Recommendation 1: Incorporate the results of iPost's monitoring of controls into key security documents such as the OpenNet security plan, security assessment report, and plan of action and milestones.

The Department does not concur with the recommendation. Although the Department appreciates the GAO's recommendation for documentation, the purpose of replacing the compliance-based security regime with one a continuous monitoring regime is to address the advanced, persistent dynamic threat that requires a continuous assessment. Successful use of metrics for prioritized attention against cyber security problems takes several forms that work together. In every category, the Department assigns a greater risk point value to a particular problem, – typically worth 10 points. Adding two No. 4 vulnerabilities risks would be tempting to compare to an 8-point risk, when adding all problems together for site or enterprise calculations. In fact, a No. 8 weakness measured in the National Vulnerability Database is far more dangerous.

To avoid this methodological problem, the State Department cubes all vulnerability risk numbers and divides by 100. Such a carefully designed mathematical strategy preserves the zero-to-10 point scales that is readily understood by everyone, but attaches an electronic strobe light to the Nos. 8, 9 and 10 risks. Cubing and dividing by 100, therefore, preserves simplicity for those working the problems and simultaneously offers a practical approach to dealing with information overload.

Recommendation 2: Document existing controls intended to ensure timeliness, accuracy, and completeness of iPost data.

The Department does not concur with the recommendation. The Department regularly evaluates the timeliness, accuracy, and completeness of the iPost data; however, further documentation is of questionable value, given the volatility of the security environment. As an example, recently the Department measured the total number of substantive changes in its network, comparing two full configurations scans 15 days apart. This calculation revealed that 150-200 significant software changes were occurring every week – a staggering 24,000 changes over a three-year period. The regrettable conclusion was that reports written to comply with security controls were prepared only as infrequently as required (once every three

years) by the applicable U.S. federal regulation. As a result, those written reports were out of date before they could be printed and placed in three-ring binders. Recommendation 3: Develop, document, and implement procedures for validating data and reviewing and reconciling output in iPost to ensure data consistency, accuracy, and completeness.

The Department concurs only partially with the recommendation. The Department has developed and implemented procedures for validating and testing output in iPost to ensure data consistency, accuracy, and completeness through its operational performance of the program. Those measures include the ones noted by the GAO: "Every Window host at each iPost site is to be scanned for vulnerabilities every seven days. The frequent collection of data helps to ensure its timeliness. In addition, State has established three scoring components – SMS Reporting, Vulnerability Reporting, and Security Compliance Reporting – in its risk scoring program to address instances when data collection tools do not correctly report the data required to compute a score for a component, such as when a host is not scanned."

Further documentation called for by the GAO would run counter to the Department's goal of avoiding an environment in which "too often we have agencies who manage what we call paper compliance rather than really addressing the security of their networks, we want to go beyond paper compliance" and effectuate meaningful security enhancements. (Quote from Senator Tom Carper in March 28, 2009, Government Information Security interview.)

Recommendation 4: Clearly identify in iPost individuals with site-level responsibility for monitoring the security state and ensuring the resolution of security weaknesses of Windows hosts.

The Department does not concur with the recommendation. Although the Department appreciates the need for accountability to be affixed to those responsible for addressing security weaknesses, the Department fails to understand the necessity for individually naming those individuals responsible for monitoring the security state and ensuring resolution of security weaknesses of Windows hosts. The Department also notes GAO's report highlights that "State officials we interviewed indicated that they reviewed iPost information on a daily basis, with one official stating it was his first task in the morning" and the "majority of State officials surveyed also indicated that iPost was very helpful in identifying Windows vulnerabilities."

Please see response to Recommendation 5.

Recommendation 5: Implement procedures to consistently notify senior managers at sites with low security grades of the need for corrective actions, in accordance with department criteria.

The Department concurs with the recommendation. The Department notifies senior managers at sites and relevant officials responsible for implementing corrective actions in accordance with Department criteria. At the end of every day, the highest average cyber score per computer and server at every location across the enterprise is the one that captures the most concern. Consistently bad scores are reported to the immediate staff of the Consul General, Ambassador, and the Assistant Secretaries once a month as a warning that their computer operations are at an especially prominent risk to their business in comparison to their peer organizations in the Department.

Recommendation 6: Develop, document, and maintain an iPost configuration management and test process.

The Department concurs only partially with the recommendation. Although the Department has maintained release notes on updates, scoring documents, and presentations on iPost, GAO asserts that "key information about the program and capabilities are not fully documented." As an example, GAO cites the lack of a "diagram of the architecture of iPost" as a deficiency. The Department fails to understand how the lack of diagram equates to a weakness in security or would allow for continuous monitoring to be addressed more effectively. Another example cited by GAO is the lack of written test plan and acceptance testing process with new releases, although GAO acknowledges that State has "improved its process for testing applications and subsequent versions of iPost."

Recommendation 7: Develop, document, and implement a continuous monitoring strategy.

The Department concurs with the recommendation. The Department will endeavor to develop, document and implement a continuous monitoring strategy with the full focus and attention a strategy of this nature deserves.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the individual named above, Ed Alexander and William Wadsworth (Assistant Directors), Carl Barden, Neil Doherty, Rebecca Eyler, Justin Fisher, Valerie Hopkins, Tammi Kalugdan, Linda Kochersberger, Karl Seifert, Michael Silver, Eugene Stevens, and Henry Sutanto made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548