

• Home

• News Topics

• Blogs

• Jobs

• Digital Communities

• Video

• Events

• Webinars

• Grants

• Magazines

• Advertise



Login

• Government Technology News

Articles

• Digital Communities

• e-Government

• Economic Stimulus

• Emergency Management

• Emerging Technologies

• Enterprise Technology

• Green Initiatives

• Products

• Public CIO

• Public Safety

2010 Cyber-Threat Forecast Sees Hacks Growing in Sophistication and Reach



SHARE

Dec 31, 2009, By [Hilton Collins, Staff Writer](#)

Comment

The new year will usher in some interesting new changes in the world of malware and cyber-attacks, according to one company's predictions for 2010.

You May Also Like

- [CSI Computer Crime and Security Survey Shows Poor Security Awareness Training in Public and Private Sectors](#)
- [White House Appoints Howard Schmidt as First Cyber-Security Coordinator](#)

Watchful eyes will have to be kept on mobile phone apps, Google Wave accounts, file sharing and peer-to-peer networks -- cyber-criminals will target those in greater numbers, according to predictions released by Kaspersky Labs, a provider of Internet threat management solutions for combating malware.

As technology touches more lives, the bad guys will see more opportunities.

- [Transportation](#)
- [Wireless](#)
- [View All News Topics...](#)

• **Get News Via Email**

• **Industry Perspectives**

- [Case Studies](#)
- [White Papers](#)
- [Partner Sites](#)

• **Government Technology Magazine**

- [Current Issue](#)
- [Subscribe](#)
- [Contact](#)



Get Govtech's
Daily Newsletter

[view sample](#)

- [Mark Weatherford: U.S. Must Protect Critical Infrastructure From Cyber-Threats](#)

Related Products

[From wireless mice to keyboards to a combo of both, we have the right wireless product for you. : Logitech](#)

[Wirelessly use keyboard, mouse and other devices with a single unifying receiver : Logitech](#)

Tools Sponsored By

"Given the growing sophistication of threats -- it's no longer just an e-mail saying, 'Please click on this attachment,' and you get infected with something -- the schemes are much more elaborate than that," said Roel Schouwenberg, the company's senior malware researcher.

Released Dec. 16, the company's predictions and findings on 2010's greatest cyber-threats and new attack vectors may be a wake-up call for some.

"A lot of things that are happening are happening invisibly, and people will not notice anything until they see that they have lost money or that their identity has been stolen," Schouwenberg said.

The forecast is divided into six predictions about the threats of tomorrow:

- more interest in attacking via Google Wave accounts as the technology is used more;
- more attacks on iPhone and Android mobile platforms as they become more popular;
- more attacks from file sharing networks instead of from Web sites

and applications;

- more mass malware epidemics being spread through peer-to-peer networks;
- less distribution of fake anti-virus programs as the market for this type of attack has been saturated and IT security professionals have been more diligent in cracking down on it; and
- more criminals providing malware traffic -- using botnets to send spam, distribute malware or performing denial-of-service attacks -- as a paid service for other criminals in subtle ways without actually committing crimes.

This means the good guys might have a tougher time fighting the good fight.

"Malware will continue to further its sophistication in 2010, with specific malware families requiring significant resources from anti-malware companies to adequately fight them," Schouwenberg said in a statement.

Although these attacks might become more pervasive, their growth could be mitigated by workplace policies that restrict or modify social networking and the usage of mobile devices while on the job.

"I'm quite sure that governments are a lot more strict about what kind of smartphones -- or phones in

generally may fall compared to the average business," Schneidewitz said. "That goes for attacks on social networks. Some government agencies have social networks blocked."

MW

1

tweet

retweet

Latest Government Technology News



- [3-D Technology Helps Emergency Responders Observe Origins of 911 Calls](#) - Apr 23
- [Florida Census Website Aims to Catch the Uncounted](#) - Apr 23
- [Adrian Farley to Lead California Office of Technology Services](#) - Apr 22
- [Open Source Document Management a Money Saver for Corpus Christi, Texas](#) - Apr 22
- [St. Petersburg, Fla., Improves Procurement Process](#) - Apr 22

[View All Government Technology News](#)

Industry Solutions for Government

Read real world deployments of technology in government from our sponsors.

- [Cyber Security Cases](#)
- [Economic Development Cases](#)
- [Enterprise Cases](#)

[View All Industry Solutions](#)



Related Products and Services



Marketplace

• [See how Adobe opens up government](#)

• [Just released. Road Map to the Virtual Data Center. FREE download.](#)

• [Corpus Christi builds a smarter city. See how in this IBM White Paper.](#)

• [Maximize IT Efficiency & Improve Return on Assets. Watch the IBM Demo.](#)

• [Effective Asset Management in an Uncertain Economy. Get the IBM White Paper.](#)

Get Govtech's Daily Newsletter

Email: [view sample](#)



Video



Roach Bots, Tweets From Space and Flower Power.

Working out the bugs by working in the cockroaches. A first for NASA. Do kids spend more time with technology than they sleep? Can sunflower seeds produce fuel for your car?



Cities Launch 311 Open Source

San Francisco Mayor Gavin Newsom announces launch of open source standard for any city to hook 311 to social networks.



Get Your Game on, Traffic Cams & Wi-Fi Cars

Will gamers be addicted to the Smithsonian Museum? California to raise \$400 million with traffic cams. Turn your car into a hotspot.

[More Video >](#)

Government Jobs

Browse hundreds of public sector career opportunities in

GovTech's new jobs section. Popular job searches:

[government IT](#), [public safety](#), [GIS](#), [transportation](#), [CIO](#), [security](#), [health](#)

Magazines: Magazine Sites, Government

Technology, Digital Communities, Public CIO,

Emergency Management, Advertise

Resources: Site Map, Search, Events,

Video, Government Articles, Slide Shows, Case

Studies, Privacy Policy, News Feeds (RSS), MyGT

Email Newsletters to Stay Informed: Executive

News, Digital Communities, Emergency

Management, Public CIO, Security, Justice and

Public Safety, Webinars.

Follow us on:  twitter

Site owned by e.Republic, Inc.

100 Blue Ravine Rd. Folsom, CA 95630.

916-932-1300 Copyright © 1995-2008. All rights reserved.

Government Technology Magazine

Government Technology Magazine provides information technology (IT) case studies, applications, news and best practices for state, city and county government.

Get FREE Subscription



GAO

Testimony

Before the Subcommittee on Government
Management, Organization, and Procurement,
Committee on Oversight and Government
Reform, U.S. House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Wednesday, March 24, 2010

INFORMATION SECURITY

**Concerted Response
Needed to Resolve
Persistent Weaknesses**

Statement of Gregory C. Wilshusen
Director, Information Security Issues



GAO

Accountability * Integrity * Reliability



INFORMATION SECURITY

Concerted Response Needed to Resolve Persistent Weaknesses

Highlights of [GAO-10-536T](#), a testimony before the Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, U.S. House of Representatives

Why GAO Did This Study

Without proper safeguards, federal computer systems are vulnerable to intrusions by individuals who have malicious intentions and can obtain sensitive information. The need for a vigilant approach to information security has been demonstrated by the pervasive and sustained cyber attacks against the United States; these attacks continue to pose a potentially devastating impact to systems as well as the operations and critical infrastructures that they support. Concerned by reports of weaknesses in federal systems, Congress passed the Federal Information Security Management Act (FISMA), which authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies.

GAO was asked to testify on federal information security and agency efforts to comply with FISMA. This testimony summarizes (1) federal agencies' efforts to secure information systems and (2) opportunities to enhance federal cybersecurity. To prepare for this testimony, GAO analyzed its prior reports and those from 24 major federal agencies, their inspectors general, and the Office of Management and Budget (OMB).

What GAO Recommends

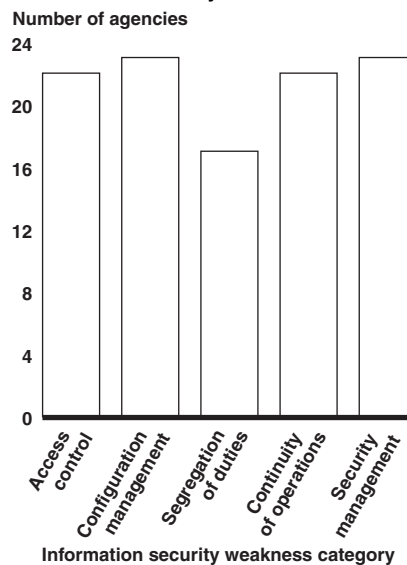
In previous reports over the past several years, GAO has made hundreds of recommendations to agencies to mitigate identified control deficiencies and to fully implement information security programs.

[View GAO-10-536T or key components.](#)
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Federal agencies have reported mixed progress in securing their systems and implementing key security activities. For example, in fiscal year 2009, agencies collectively reported an increasing percentage of personnel receiving security awareness training and specialized security training, but a decreasing rate of implementation for other key activities when compared to fiscal year 2008. In addition, federal systems continued to be afflicted by persistent control weaknesses. Almost all of the 24 major federal agencies had information security weaknesses in five key control categories, as illustrated in the figure below.

Information Security Weaknesses at Major Federal Agencies for Fiscal Year 2009



Source: GAO analysis of IG, agency, and GAO reports.

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements of an agencywide information security program, as required by FISMA. As a result, they may be at increased risk of unauthorized disclosure, modification, and destruction of information or disruption of mission critical operations. Such risks are illustrated, in part, by the increasing number of security incidents experienced by federal agencies.

Opportunities exist to enhance federal cybersecurity through a concerted response to safeguarding systems that include several components. First, agencies can implement the hundreds of recommendations GAO and inspectors general have made to resolve control deficiencies and information security program shortfalls. In addition, OMB's continued efforts to improve reporting and oversight as recommended by GAO could help assess agency programs. Finally, the White House, OMB, and certain federal agencies have undertaken several governmentwide initiatives that are intended to enhance information security at federal agencies.

Chairwoman Watson and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing on federal information security. As the number of reported computer security incidents and threats to the nation's cyber infrastructure steadily increase, the need for a vigilant and comprehensive approach to federal information security is greater than ever. In 2009, the federal government faced coordinated attacks against its Web sites, and several agencies were affected by the Gumbler Trojan, which uses multiple exploits to compromise legitimate web pages. In addition, the Conficker worm posed a threat to both federal and non-federal systems. Such attacks highlight the importance of developing a concerted response to safeguard federal information systems.

Proper safeguards can mitigate the risk to federal computer systems and networks posed by individuals and groups with malicious intentions. While progress has been made in identifying and implementing these controls, much work remains. Over the past few years, federal agencies have reported numerous security incidents in which sensitive information has been lost or stolen, including personally identifiable information, which has exposed millions of Americans to the loss of privacy, identity theft, and other financial crimes.

In my testimony today, I will discuss (1) federal agencies' efforts to secure information systems and (2) opportunities to enhance federal cybersecurity. In conducting our review, we analyzed agency, inspector general, Office of Management and Budget (OMB), and our reports on information security. We conducted the review from December 2009 to March 2010 in the Washington, D.C., area 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.

Background

To help protect against threats to federal systems, the Federal Information Security Management Act (FISMA)¹ is intended to set forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. Its framework creates a cycle of risk management activities necessary for an effective security program; these activities are similar to the principles noted in our study of the risk management activities of leading private sector organizations²—assessing risk, establishing a central management focal point, implementing appropriate policies and procedures, promoting awareness, and monitoring and evaluating policy and control effectiveness.

In order to ensure the implementation of this framework, FISMA assigns specific responsibilities to (1) agency heads and chief information officers, to develop, document, and implement an agencywide information security program, among other things; (2) inspectors general, to conduct annual independent evaluations of agency efforts to effectively implement information security; (3) the National Institute for Science and Technology (NIST), to provide standards and guidance to agencies on information security; and (4) OMB, which include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security and reviewing, at least annually, and approving or disapproving, agency information security programs. In addition, the act requires each agency to report annually to OMB, selected congressional committees, and the Comptroller General on the adequacy of its information security policies, procedures, practices, and compliance with requirements. FISMA also requires OMB to report annually to Congress by March 1.

¹FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No.107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

²GAO, *Executive Guide: Information Security Management: Learning from Leading Organizations*, [GAO/AIMD-98-68](#) (Washington, D.C.: May 1998).

Although Agencies Report Mixed Progress, Deficiencies in Information Security Controls Remain

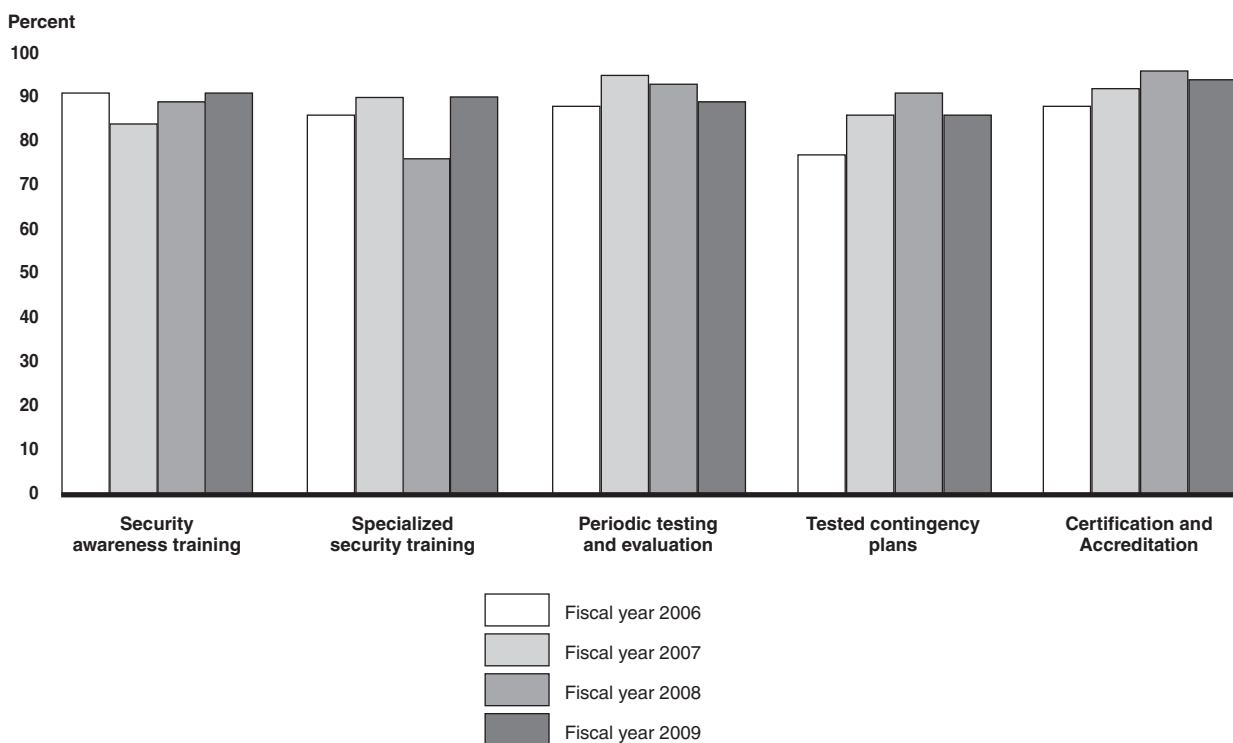
FISMA requires each agency, including agencies with national security systems, to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. As part of its oversight responsibilities OMB requires agencies to report on specific performance measures, including:

- Percentage of employees and contractors receiving IT security awareness training,
- Percentage of employees with significant security responsibilities who received specialized security training,
- Percentage of systems whose controls were tested and evaluated,
- Percentage of systems with tested contingency plans, and
- Percentage of systems certified and accredited.

Since the enactment of FISMA in 2002, federal agencies have generally reported increasing rates of implementation for key information security activities. However, in fiscal year 2009, agencies reported mixed progress in implementing these activities compared to fiscal year 2008. For example, governmentwide, agencies collectively reported that 91 percent of employees and contractors had received security awareness training in fiscal year 2009, up from 89 percent in fiscal year 2008. Agencies also reported that 90 percent of employees with significant information security responsibilities had received specialized training, up from 76 percent in fiscal year 2008.

In other key areas, agencies reported slight decreases from fiscal years 2008 to 2009. Specifically, the percentage of systems for which security controls have been tested and reviewed decreased from 93 percent to 89 percent, the percentage of systems with tested contingency plans decreased from 91 percent to 86 percent, and the percentage of systems certified and accredited decreased from 96 percent to 94 percent. A summary of these percentages is shown in figure 1.

Figure 1: Selected Performance Metrics for Agency Systems



Source: GAO analysis of agency data.

In these and other areas, inspectors general at the 24 major agencies have also reported weaknesses in their fiscal year 2009 audits and evaluations. Weaknesses in requirements such as periodic testing and evaluation, certification and accreditation, configuration management, and remedial actions were most commonly reported. For example,

- at least 13 inspectors general reported that their agencies had insecure configuration settings, or had not applied needed patches in a timely manner, or both;
- at least 15 inspectors general reported that their agency did not adequately assess security controls such as those recommended by NIST;
- at least 11 inspectors general reported that their agencies failed to create a remediation plan for all identified weaknesses.
- at least 13 inspectors general reported that documents required to make an informed decision regarding certification and accreditation of systems

were either missing or incomplete, or that the accreditation was allowed to expire on at least one system without recertification;

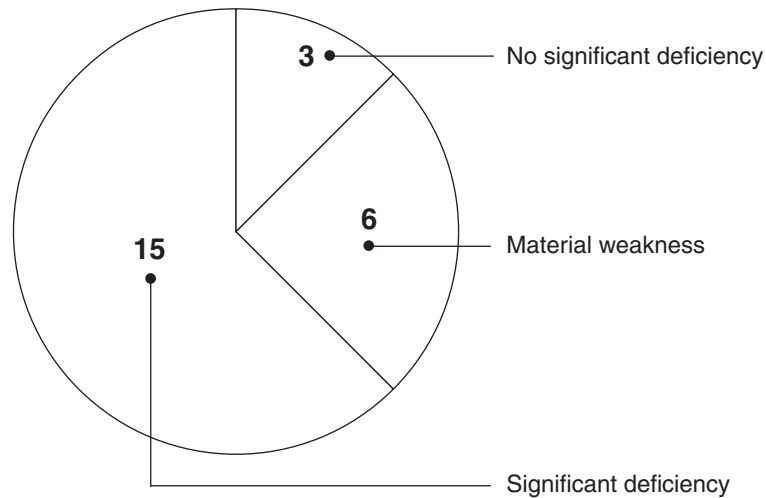
Weaknesses such as these continue to impair the government's ability to ensure the confidentiality, integrity, and availability of critical information and information systems used to support the operations and assets of federal agencies. Until these agencies fully implement information security requirements, they may be at increased risk of unauthorized disclosure, modification, and destruction of information or disruption of mission critical operations.

Despite Reported Progress, Federal Systems Remain Vulnerable

GAO and agency inspectors general reviews continue to highlight deficiencies in the implementation of security policies and procedures at federal agencies. In their fiscal year 2009 performance and accountability reports, 21 of 24 major agencies noted that inadequate information system controls over their financial systems and information were either a material weakness or a significant deficiency (see fig. 2).³

³A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

Figure 2: Number of Major Agencies Reporting Significant Deficiencies in Information Security for Financial Reporting



Source: GAO analysis of agency performance and accountability report, annual financial report, or other financial statement reports for FY 2009.

Our audits and those of the inspectors general continue to identify similar conditions in both financial and non-financial systems. Most of the 24 major federal agencies had reported deficiencies in the following major categories of information security controls, as defined by our *Federal Information System Controls Audit Manual*:⁴

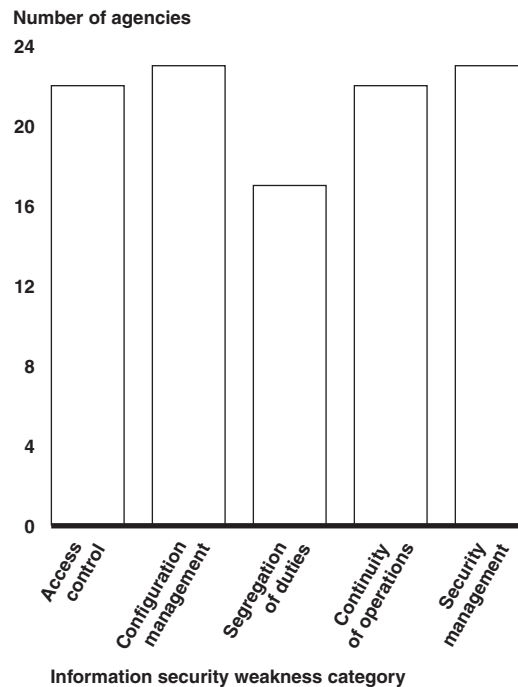
- access controls, which ensure that only authorized individuals can read, alter, or delete data;
- configuration management controls, which provide assurance that only authorized software programs are implemented;
- segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection;
- continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and

⁴GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: Feb. 2009).

- an agencywide information security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented.

As shown in figure 3, agencies reported deficiencies in all five of the information security control areas. For example, agencies did not consistently configure network devices and services to prevent unauthorized access and ensure system integrity; assign incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction; and maintain or test continuity of operations plans for key information systems. Such information security control weaknesses unnecessarily increase the risk that the reliability and availability of data that are recorded in or transmitted by federal systems could be compromised.

Figure 3: Number of Major Agencies Reporting Weaknesses by Control Category for Fiscal Year 2009



Source: GAO analysis of IG, agency, and GAO reports.

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements of an agencywide information security program, as required

by FISMA. An agencywide security program provides a framework and continuing cycle of activity that includes assessing and managing risk, developing and implementing security policies and procedures, promoting security awareness and training, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. According to inspector general, agency, and our previous reports, 23 of the 24 major federal agencies had weaknesses in their agencywide information security programs.

The following examples, reported in 2009, illustrate that a broad array of federal information and systems remain at risk.

- At the Financial Crimes Enforcement Network (FinCEN), a bureau within the Department of the Treasury, key information security program activities were not implemented.⁵ For example, FinCEN did not always include detailed implementation guidance in its policies and procedures or adequately test and evaluate information security controls.
- The information security program for the classified computer network at the Los Alamos National Laboratory (LANL) had not been fully implemented.⁶ Specifically, (1) risk assessments were not comprehensive, (2) specific guidance was missing from policies and procedures, (3) the training and awareness program did not adequately address specialized training needs for individuals with significant network security responsibilities, (4) system security plans were incomplete, (5) the system security testing and evaluation process had shortcomings, (6) corrective action plans were not comprehensive, and (7) contingency plans were incomplete and not tested. In addition, the laboratory's decentralized management approach has led to weaknesses in the effectiveness of its classified cybersecurity program. Although the laboratory has taken steps to address these weaknesses, its efforts may be limited because LANL has not demonstrated a consistent capacity to sustain security improvements over the long term.

⁵GAO, *Information Security: Further Actions Needed to Address Risks to Bank Secrecy Act Data*, [GAO-09-195](#) (Washington, D.C.: Jan. 30, 2009).

⁶GAO, *Information Security: Actions Needed to Better Manage, Protect, and Sustain Improvements to Los Alamos National Laboratory's Classified Computer Network*, [GAO-10-28](#) (Washington, D.C.: Oct. 14, 2009).

-
- We identified a number of shortcomings in key program activities at the National Aeronautics and Space Administration (NASA).⁷ For example, NASA had not always (1) fully assessed information security risks; (2) fully developed and documented security policies and procedures; (3) included key information in security plans; (4) conducted comprehensive tests and evaluation of its information system controls; (5) tracked the status of plans to remedy known weaknesses; (6) planned for contingencies and disruptions in service; (7) maintained capabilities to detect, report, and respond to security incidents; and (8) incorporated important security requirements in its agreement with its contractor.

In addition, the inspectors general at 13 of the 24 major agencies reported information security as major management challenge. Due to the persistent nature of information security vulnerabilities and the associated risks, we continue to designate information security as a governmentwide high-risk issue in our most recent biennial report to Congress; a designation we have made in each report since 1997.⁸

Reported Security Incidents Are on the Rise

Consistent with the evolving and growing nature of the threats and persistent vulnerabilities to federal systems, agencies are reporting an increasing number of security incidents and events. These incidents put sensitive information at risk. Personally identifiable information about Americans has been lost, stolen, or improperly disclosed, thereby potentially exposing those individuals to loss of privacy, identity theft, and financial crimes. Reported attacks and unintentional incidents involving critical infrastructure systems demonstrate that a serious attack could be devastating. Agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices.

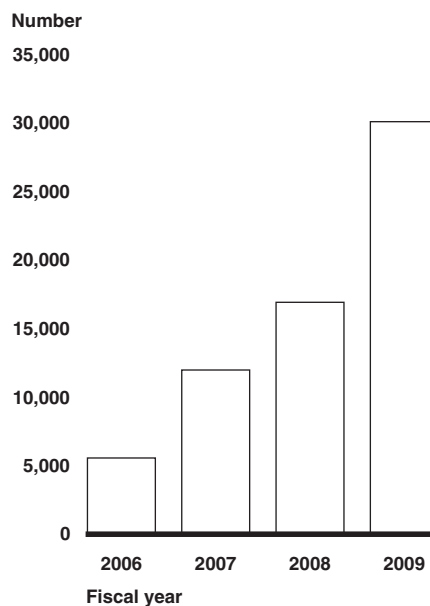
When incidents occur, agencies are to notify the federal information security incident center—the United States Computer Emergency Readiness Team (US-CERT). US-CERT serves as a focal point for the government’s interaction with federal and nonfederal entities on a 24-hour-a-day, 7-day-a-week basis regarding cyber-related analysis, warning,

⁷GAO, *Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks*, [GAO-10-4](#) (Washington, D.C.: Oct. 15, 2009).

⁸Most recently, GAO, *High-Risk Series: An Update*, [GAO-09-271](#) (Washington, D.C.: January 2009).

information sharing, major incident response, and national-level recovery efforts. As shown in figure 4, the number of incidents reported by federal agencies to US-CERT has increased dramatically over the past 4 years, increasing from 5,503 incidents reported in fiscal year 2006 to about 30,000 incidents in fiscal year 2009 (over a 400 percent increase).

Figure 4: Incidents Reported to US-CERT, FY 2006-2009



Source: GAO analysis of US-CERT data.

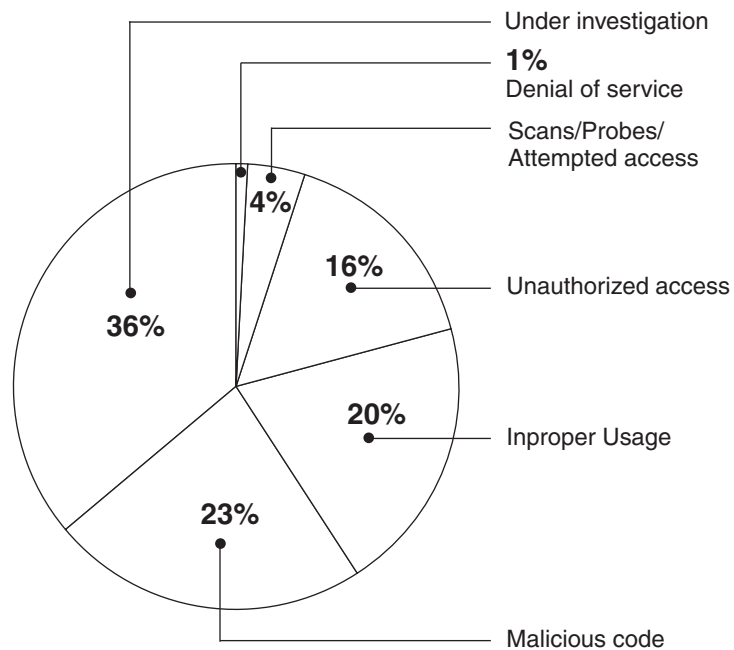
Agencies report the following types of incidents and events based on US-CERT-defined categories:

- **Unauthorized access:** Gaining logical or physical access without permission to a federal agency's network, system, application, data, or other resource.
- **Denial of service:** Preventing or impairing the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim of or participating in a denial of service attack.
- **Malicious code:** Installing malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are not required to report malicious logic that has been successfully quarantined by antivirus software.

- **Improper usage:** Violating acceptable computing use policies.
- **Scans/probes/attempted access:** Accessing or identifying a federal agency computer, open ports, protocols, service, or any combination of these for later exploit. This activity does not directly result in a compromise or denial of service.
- **Unconfirmed incidents under investigation:** Investigating unconfirmed incidents that are potentially malicious, or anomalous activity deemed by the reporting entity to warrant further review.

The four most prevalent types of incidents and events reported to US-CERT during fiscal year 2009 were: (1) malicious code comprising 23 percent; (2) improper usage, 20 percent; (3) unauthorized access, 16 percent; and (4) unconfirmed incidents under investigation, 36 percent. Incidents reported to US-CERT in fiscal year 2009 are shown by type in figure 5.

Figure 5: Percentage of Incidents Reported to US-CERT in Fiscal Year 2009 by Category



Source: GAO analysis of U.S. CERT data.

Opportunities Exist for Enhancing Federal Cybersecurity

A concerted response to safeguarding federal systems includes several components. Agencies can take action to resolve specific security weaknesses, federal law and guidance can be strengthened, and continued effort can be made on governmentwide security initiatives.

Over the past several years, we and agency inspectors general have made hundreds of recommendations to resolve significant control deficiencies and information security program shortfalls. Effective implementation of our recommendations will help agencies to prevent, limit, and detect unauthorized access to computerized networks and systems and help ensure that only authorized individuals can read, alter, or delete data. In addition, implementation of these recommendations will help agencies to better manage the configuration of security features for hardware and software and assure that changes to the configuration are systematically controlled.

We have also recommended that agencies fully implement comprehensive, agencywide information security programs, including by correcting weaknesses in specific areas of their programs such as: (1) assessments of the risk to information systems; (2) information security policies and procedures; (3) planning for interruptions to information system processing; (4) training personnel in awareness of security policies and procedures; (5) periodic tests and evaluations of the effectiveness of information system controls; and (6) the implementation of plans of action to remediate information security weaknesses. The effective implementation of these recommendations will strengthen the security posture at these agencies. Agencies have implemented or are in the process of implementing many of our recommendations.

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. Because federal computing environments are very large, complex, and geographically dispersed, often consisting of tens or hundreds of thousands of devices, increasing automation of key security processes can assist in the efficient and effective implementation of key controls across the entire enterprise. 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. In addition, improving the use of automated tools for patch management can increase

efficiency in mitigating known vulnerabilities on many systems within an agency.

Strengthen FISMA and Its Implementing Guidance

FISMA was intended to provide (1) a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets and (2) a mechanism for improved oversight of federal agency information security programs. In June 2009,⁹ we proposed several suggested actions that could improve FISMA and its associated implementing guidance, including (1) clarifying requirements for testing and evaluating security controls; (2) requiring agency heads to provide an assurance statement on the overall adequacy and effectiveness of the agency's information security program; (3) enhancing independent annual evaluations; (4) strengthening annual reporting mechanisms; and (5) strengthening OMB oversight of agency information security programs. Implementing these suggestions can improve the implementation and oversight of federal agency information security programs.

Continue Efforts to Improve Reporting and Oversight

FISMA specifies that OMB is to develop policies, principles, standards, and guidelines on information security. Each year, OMB provides instructions to federal agencies and their inspectors general for preparing the annual FISMA reports. OMB developed an online reporting tool during fiscal year 2009 to improve the efficiency of the annual reporting process. Agencies are required to use the online tool to submit their annual reports and OMB is to use the data submitted in its online reporting tool to summarize the information provided by the agencies and the inspectors general in its report to Congress.

We have previously made several recommendations to OMB for improving its annual reporting instructions and oversight.¹⁰ For example, we have recommended that OMB update its annual reporting instructions to request inspectors general report on the effectiveness of agencies'

⁹GAO, *Federal Information Security Issues*, [GAO-09-817R](#) (Washington, D.C.: June 30, 2009).

¹⁰GAO, *Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses*, [GAO-09-546](#) (Washington, D.C.: July 17, 2009) and *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, [GAO-07-837](#) (Washington, D.C.: July 27, 2007).

processes for developing inventories, monitoring contractor operations, and providing specialized security training. OMB has acted to enhance its reporting instructions; however, further actions need to be taken to fully address these recommendations.

We have also recommended that OMB develop metrics that (1) focus on the effectiveness of information security controls and (2) the overall impact of an agency's information security program.¹¹ In September 2009, OMB convened a Security Metrics Taskforce to develop new FISMA performance measures. According to OMB's website the taskforce is comprised of officials from the both the federal community and private sector and was tasked with developing metrics that focus on outcomes rather than compliance that agencies will be required to report as part of the FISMA reporting process. In December 2009, OMB released draft metrics for comment but has not yet released the final metrics.

Continue to Enhance Federal Information Security through Governmentwide Initiatives

The White House, OMB, and certain federal agencies have undertaken several governmentwide initiatives that are intended to enhance information security at federal agencies.

Address challenges in implementing CNCI. In January 2008, President Bush established the Comprehensive National Cybersecurity Initiative (CNCI). The initiative, which consists of 12 projects, is intended to reduce vulnerabilities, protect against intrusions, and anticipate future threats against federal executive branch information systems.¹² As we recently reported,¹³ the White House and federal agencies have established interagency groups to plan and coordinate CNCI activities. However, CNCI faces challenges in achieving its objectives related to securing federal information, including better defining agency roles and responsibilities, establishing measures of effectiveness, and establishing an appropriate level of transparency. Until these challenges are adequately addressed, there is a risk that CNCI will not fully achieve its goals. Among other

¹¹GAO, *Information Security: Concerted Effort Needed to Improve Federal Performance Measures*, [GAO-09-617](#) (Washington, D.C.: Sep. 14, 2009).

¹²The White House, National Security Presidential Directive 54/ Homeland Security Presidential Directive 23 (Washington, D.C.: Jan. 8, 2008).

¹³GAO, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, [GAO-10-338](#) (Washington, D.C.: March 5, 2010).

recommendations, we recommended that the Director of OMB take action to: (1) better define roles and responsibilities of all key CNCI participants; (2) establish measures to determine the effectiveness of CNCI projects in making federal information systems more secure and track progress against those measures; (3) establish an appropriate level of transparency about CNCI; and (4) reach agreement on the scope of CNCI's education projects to ensure that an adequate cadre of skilled personnel is developed to protect federal information systems. OMB agreed with 3 of the 4 recommendations, disagreeing with the recommendation regarding defining roles and responsibilities. However, such definitions are key to achieving CNCI's objective of securing federal systems.

Continue efforts to implement TIC and Einstein initiatives. Two specific initiatives of CNCI are Trusted Internet Connections (TIC) and Einstein. TIC is an effort to consolidate the federal government's external access points (including those to the Internet). TIC is also intended to establish baseline security capabilities and validate agency adherence to those security capabilities. The Einstein initiative is a computer network intrusion detection system that analyzes network flow information from participating federal agencies. The system is to provide a high-level perspective from which to observe potential malicious activity in computer network traffic of participating agencies' computer networks. Einstein is intended to alert US-CERT in real time of this activity and provides correlation and visualization of the derived data. We have ongoing work that addresses status and implementation of these initiatives.

Continue efforts to implement FDCC. Under the Federal Desktop Core Configuration Initiative, OMB directed agencies that have Windows XP and/or Windows Vista operating systems deployed to adopt the security configurations developed by the National Institute of Standards and Technology, the Department of Defense, and DHS. The goal of this initiative is to improve information security and reduce overall information technology operating costs. We have ongoing work that addresses status and implementation of this initiative.

Improve the national strategy for cybersecurity. In March 2009, we testified on needed improvements to the nation's cybersecurity strategy.¹⁴

¹⁴GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, [GAO-09-432T](#) (Washington, D.C.: March 10, 2009).

In preparation for that testimony, we obtained the views of experts (by means of panel discussions) on critical aspects of the strategy, including areas for improvement. The experts, who included former federal officials, academics, and private sector executives, highlighted 12 key improvements that are, in their view, essential to improving the strategy and our national cybersecurity posture. The key strategy improvements identified by cybersecurity experts are listed in table 1.

Table 1: Key Strategy Improvement Identified by Cybersecurity Experts

1. Develop a national strategy that clearly articulates strategic objectives, goals, and priorities.
2. Establish White House responsibility and accountability for leading and overseeing national cybersecurity policy.
3. Establish a governance structure for strategy implementation.
4. Publicize and raise awareness about the seriousness of the cybersecurity problem.
5. Create an accountable, operational cybersecurity organization.
6. Focus more actions on prioritizing assets, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.
7. Bolster public-private partnerships through an improved value proposition and use of incentives.
8. Focus greater attention on addressing the global aspects of cyberspace.
9. Improve law enforcement efforts to address malicious activities in cyberspace.
10. Place greater emphasis on cybersecurity research and development, including consideration of how to better coordinate government and private sector efforts.
11. Increase the cadre of cybersecurity professionals.
12. Make the federal government a model for cybersecurity, including using its acquisition function to enhance cybersecurity aspects of products and services.

Source: GAO analysis of opinions solicited during expert panels.

These recommended improvements to the national strategy are in large part consistent with our previous reports and extensive research and experience in this area. Until they are addressed, our nation's most critical federal and private sector cyber infrastructure remain at unnecessary risk to attack from our adversaries.

Since our March testimony, the Obama Administration has performed a review¹⁵ of the strategy and issued a list of short and long term actions,

¹⁵The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

which are largely consistent with our past reports and recommendations, to strengthen the strategy. In response to one of these actions, the president appointed a cybersecurity coordinator in December 2009. We recently initiated a review to assess the progress made by the executive branch in implementing the report's recommendations.

In summary, while federal agencies continue to report increased compliance in implementing security training requirements, most federal agencies reported weaknesses in most types of information security controls. Additionally, agencies reported mixed progress in implementing key security measures while inspectors general identified persistent weaknesses in those areas of agencies' information security programs. There are multiple opportunities for the federal government to enhance federal cybersecurity and address these continuing weaknesses. These opportunities include addressing the hundreds of recommendations we and inspectors general have made to agencies, making enhancements to FISMA and its implementing guidance, and continuing efforts on White House, OMB, and federal agencies' initiatives. A concerted response by the federal government to current information security challenges will include acting on these opportunities; without such a response, federal information and systems will remain vulnerable.

Chairwoman Watson, this concludes my statement. I would be happy to answer any questions you or other members of the subcommittee may have.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this statement include Anjalique Lawrence (Assistant Director), Larry Crosland, Sharhonda Deloach, Kristi Dorsey, Rebecca Eyler, Nicole Jarvis, Linda Kochersberger, Mary Marshall, Minette Richardson, and Jayne Wilson.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

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





Testimony
Before the Subcommittee on
Government Management, Organization,
and Procurement; House Committee on
Oversight and Government Reform

For Release on Delivery
Expected at time 2:00 p.m. EDT
May 5, 2009

**INFORMATION
SECURITY**

**Cyber Threats and
Vulnerabilities Place
Federal Systems at Risk**

Statement of Gregory C. Wilshusen,
Director, Information Security Issues



G A O

Accountability * Integrity * Reliability



Highlights of [GAO-09-661T](#), a testimony before the Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where maintaining the public's trust is essential. The need for a vigilant approach to information security has been demonstrated by the pervasive and sustained computer-based (cyber) attacks against the United States and others that continue to pose a potentially devastating impact to systems and the operations and critical infrastructures that they support.

GAO was asked to describe (1) cyber threats to federal information systems and cyber-based critical infrastructures and (2) control deficiencies that make these systems and infrastructures vulnerable to those threats. To do so, GAO relied on its previous reports and reviewed agency and inspectors general reports on information security.

What GAO Recommends

In previous reports over the past several years, GAO has made hundreds of recommendations to agencies to mitigate identified control deficiencies and to fully implement information security programs.

View [GAO-09-661T](#) or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

INFORMATION SECURITY

Cyber Threats and Vulnerabilities Place Federal Systems at Risk

What GAO Found

Cyber threats to federal information systems and cyber-based critical infrastructures are evolving and growing. These threats can be unintentional and intentional, targeted or nontargeted, and can come from a variety of sources, such as foreign nations engaged in espionage and information warfare, criminals, hackers, virus writers, and disgruntled employees and contractors working within an organization. Moreover, these groups and individuals have a variety of attack techniques at their disposal, and cyber exploitation activity has grown more sophisticated, more targeted, and more serious. As government, private sector, and personal activities continue to move to networked operations, as digital systems add ever more capabilities, as wireless systems become more ubiquitous, and as the design, manufacture, and service of information technology have moved overseas, the threat will continue to grow. In the absence of robust security programs, agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices. These developments have led government officials to become increasingly concerned about the potential for a cyber attack.

According to GAO reports and annual security reporting, federal systems are not sufficiently protected to consistently thwart cyber threats. Serious and widespread information security control deficiencies continue to place federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. For example, over the last several years, most agencies have not implemented controls to sufficiently prevent, limit, or detect access to computer networks, systems, and information, and weaknesses were reported in such controls at 23 of 24 major agencies for fiscal year 2008. Agencies also did not always configure network devices and service properly, segregate incompatible duties, or ensure that continuity of operations plans contained all essential information. An underlying cause for these weaknesses is that agencies have not yet fully or effectively implemented key elements of their agencywide information security programs. To improve information security, efforts have been initiated that are intended to strengthen the protection of federal information and information systems. For example, the Comprehensive National Cybersecurity Initiative was launched in January 2008 and is intended to improve federal efforts to protect against intrusion attempts and anticipate future threats. Until such opportunities are seized and fully exploited and GAO recommendations to mitigate identified control deficiencies and implement agencywide information security programs are fully and effectively implemented, federal information and systems will remain vulnerable.

Chairwoman Watson and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing on the threats, vulnerabilities, and challenges in securing federal information systems. Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where maintaining the public's trust is essential. The need for a vigilant approach to information security has been demonstrated by the pervasive and sustained computer-based (cyber) attacks against the United States and others that continue to pose a potentially devastating impact to systems and the operations and critical infrastructures that they support.

In my testimony today, I will describe (1) cyber threats to federal information systems and cyber-based critical infrastructures and (2) control deficiencies that make these systems and infrastructures vulnerable to those threats. In preparing for this testimony, we relied on our previous reports on federal information security. These reports contain detailed overviews of the scope and methodology we used. We also reviewed inspectors general (IG) reports on information security, analyzed performance and accountability reports for 24 major federal agencies,¹ and examined information provided by the U.S. Computer Emergency Readiness Team (US-CERT) on reported security incidents.

We conducted our work in support of this testimony during April and May 2009, in the Washington, D.C. area. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate

¹The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs, the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

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.

Background

As computer technology has advanced, federal agencies have become dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions, deliver services to the public, and account for their resources without these information assets. Information security is thus especially important for federal agencies to ensure the confidentiality, integrity, and availability of their information and information systems. Conversely, ineffective information security controls can result in significant risk to a broad array of government operations and assets. For example:

- Resources, such as federal payments and collections, could be lost or stolen.
- Computer resources could be used for unauthorized purposes or to launch attacks on other computer systems.
- Sensitive information, such as taxpayer data, Social Security records, medical records, intellectual property, and proprietary business information, could be inappropriately disclosed, browsed, or copied for purposes of identity theft, espionage, or other types of crime.
- Critical operations, such as those supporting critical infrastructure, national defense, and emergency services, could be disrupted.
- Data could be added, modified, or deleted for purposes of fraud, subterfuge, or disruption.

-
- Agency missions could be undermined by embarrassing incidents that result in diminished confidence in the ability of federal organizations to conduct operations and fulfill their responsibilities.

Federal Systems and Infrastructures Face Increasing Cyber Threats

Cyber threats to federal information systems and cyber-based critical infrastructures are evolving and growing. In September 2007, we reported² that these threats can be unintentional and intentional, targeted or nontargeted, and can come from a variety of sources. Unintentional threats can be caused by inattentive or untrained employees, software upgrades, maintenance procedures, and equipment failures that inadvertently disrupt systems or corrupt data. Intentional threats include both targeted and nontargeted attacks. A targeted attack is when a group or individual attacks a specific system or cyber-based critical infrastructure. A nontargeted attack occurs when the intended target of the attack is uncertain, such as when a virus, worm, or other malicious software³ is released on the Internet with no specific target.

Government officials are concerned about attacks from individuals and groups with malicious intent, such as criminals, terrorists, and adversarial foreign nations. For example, in February 2009, the Director of National Intelligence testified that foreign nations and criminals have targeted government and private sector networks to gain a competitive advantage and potentially disrupt or destroy them, and that terrorist groups have expressed a desire to use cyber attacks as a means to target the United States.⁴ The Federal Bureau of Investigation has identified multiple sources of threats to our

²GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, [GAO-07-1036](#) (Washington, D.C.: Sept. 10, 2007).

³“Malware” (malicious software) is defined as programs that are designed to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs so that users are induced into activating them.

⁴Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

nation’s critical information systems, including foreign nations engaged in espionage and information warfare, domestic criminals, hackers, virus writers, and disgruntled employees and contractors working within an organization. Table 1 summarizes those groups or individuals that are considered to be key sources of cyber threats to our nation’s information systems and cyber infrastructures.

Table 1: Sources of Cyber Threats

Threat source	Description
Foreign nations	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. According to the Director of National Intelligence, a growing array of state and nonstate adversaries are increasingly targeting—for exploitation and potentially disruption or destruction—information infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. ^a
Criminal groups	There is an increased use of cyber intrusions by criminal groups that attack systems for monetary gain.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, attack tools have become more sophisticated and easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Disgruntled insiders	The disgruntled insider, working from within an organization, is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes contractor personnel.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. However, traditional terrorist adversaries of the United States are less developed in their computer network capabilities than other adversaries. Terrorists likely pose a limited cyber threat. The Central Intelligence Agency believes terrorists will stay focused on traditional attack methods, but it anticipates growing cyber threats as a more technically competent generation enters the ranks.

Source: Federal Bureau of Investigation, unless otherwise indicated.

^a Prepared statement of Dennis Blair, Director of Central Intelligence, before the Senate Select Committee on Intelligence, February 12, 2009.

These groups and individuals have a variety of attack techniques at their disposal. Furthermore, as we have previously reported,⁵ the

⁵GAO, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07-705 (Washington, D.C.: June 22, 2007).

techniques have characteristics that can vastly enhance the reach and impact of their actions, such as the following:

- Attackers do not need to be physically close to their targets to perpetrate a cyber attack.
- Technology allows actions to easily cross multiple state and national borders.
- Attacks can be carried out automatically, at high speed, and by attacking a vast number of victims at the same time.
- Attackers can more easily remain anonymous.

Table 2 identifies the types and techniques of cyber attacks that are commonly used.⁶

Table 2: Types and Techniques of Cyber Attacks

Type of attack	Description
Denial of service	A method of attack that denies system access to legitimate users without actually having to compromise the targeted system. From a single source, the attack overwhelms the target computers with messages and blocks legitimate traffic. It can prevent one system from being able to exchange data with other systems or prevent the system from using the Internet.
Distributed denial of service	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Exploit tools	Publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Logic bomb	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Trojan horse	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.
Virus	A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected files is loaded into memory, allowing the virus to infect other files. Unlike the computer worms, a virus requires human involvement (usually unwitting) to propagate.

⁶GAO-07-705 and GAO, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*, GAO-04-321 (Washington, D.C.: May 28, 2004).

Type of attack	Description
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
Spyware	Malware installed without the user's knowledge to surreptitiously track and/or transmit data to an unauthorized third party.
War-dialing	Simple program that dial consecutive phone numbers looking for a modem.
War-driving	A method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adaptor that involves patrolling locations to gain unauthorized access.
Spamming	Sending unsolicited commercial e-mail advertising for products, services, and Web sites. Spam can also be used as a delivery mechanism for malicious software and other cyber threats.
Phishing	A high-tech scam that frequently uses spam or pop-up messages to deceive people into disclosing sensitive information. Internet scammers use e-mail bait to "phish" for passwords and financial information from the sea of internet users.
Spoofing	Creating a fraudulent Web site to mimic an actual, well-known site run by another party. E-mail spoofing occurs when the sender address and other parts of an e-mail header are altered to appear as though the e-mail originated from a different source. Spoofing hides the origin of an e-mail message.
Pharming	A method used by phishers to deceive users into believing that they are communicating with a legitimate Web site. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed Web site when the user types a legitimate Web address.
Botnet	A network of remotely controlled systems used to coordinate attacks and distribute malware, spam, and phishing scams. Bots (short for "robots") are programs that are covertly installed on a targeted system allowing an unauthorized user to remotely control the compromised computer for a variety of malicious purposes.

Source: GAO.

Government officials are increasingly concerned about the potential for a cyber attack. According to the Director of National Intelligence,⁷ the growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, and other critical infrastructures. As government, private sector, and personal activities continue to move to networked operations, as digital systems add ever more capabilities, as wireless systems become more ubiquitous, and as the design, manufacture, and service of IT have moved overseas, the threat will continue to grow. Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious. For example, the Director of National Intelligence also stated that, in August 2008, the Georgian national government's Web sites were disabled during hostilities with Russia, which hindered the government's ability to

⁷Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

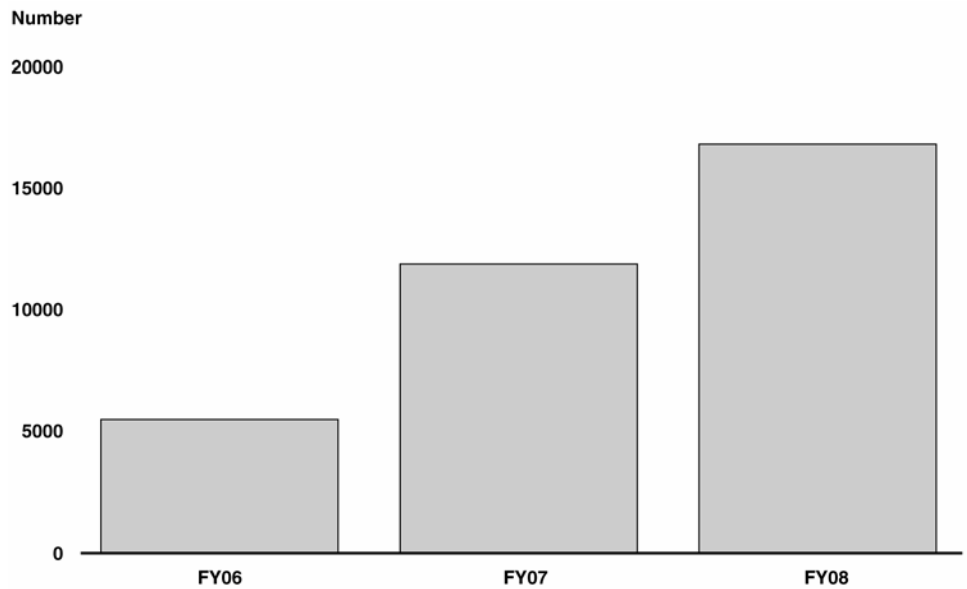
communicate its perspective about the conflict. The director expects disruptive cyber activities to become the norm in future political and military conflicts.

Reported Security Incidents Are on the Rise

Perhaps reflective of the evolving and growing nature of the threats to federal systems, agencies are reporting an increasing number of security incidents. These incidents put sensitive information at risk. Personally identifiable information about Americans has been lost, stolen, or improperly disclosed, thereby potentially exposing those individuals to loss of privacy, identity theft, and financial crimes. Reported attacks and unintentional incidents involving critical infrastructure systems demonstrate that a serious attack could be devastating. Agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices.

When incidents occur, agencies are to notify the federal information security incident center—US-CERT. As shown in figure 1, the number of incidents reported by federal agencies to US-CERT has increased dramatically over the past 3 years, increasing from 5,503 incidents reported in fiscal year 2006 to 16,843 incidents in fiscal year 2008 (about a 206 percent increase).

Figure 1: Incidents Reported to US-CERT in Fiscal Years 2006 through 2008



Source: GAO analysis of US-CERT data.

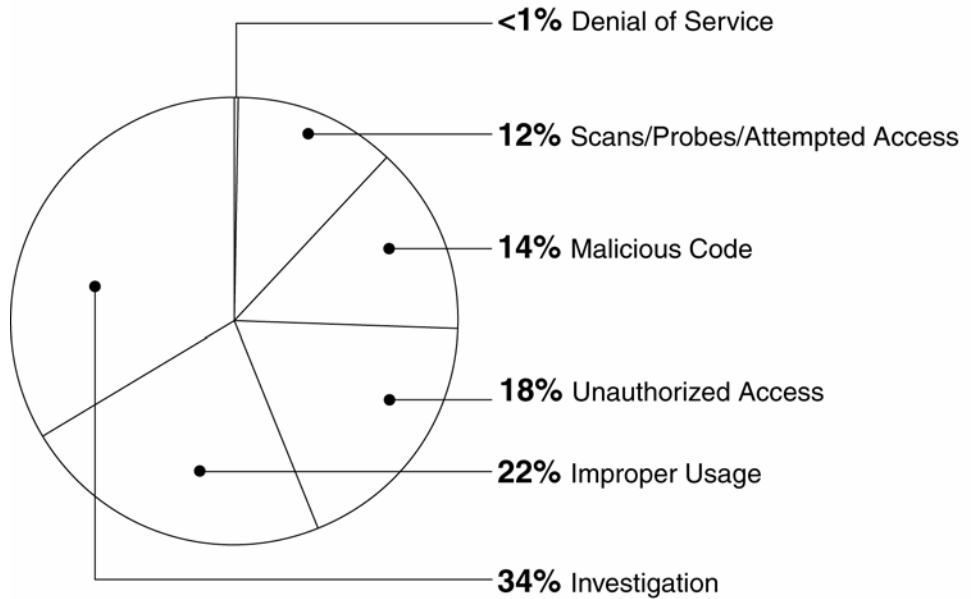
Incidents are categorized by US-CERT in the following manner:

- **Unauthorized access:** In this category, an individual gains logical or physical access without permission to a federal agency's network, system, application, data, or other resource.
- **Denial of service:** An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in a denial of service attack.
- **Malicious code:** Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are not required to report malicious logic that has been successfully quarantined by antivirus software.
- **Improper usage:** A person violates acceptable computing use policies.

- Scans/probes/attempted access: This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination of these for later exploit. This activity does not directly result in a compromise or denial of service.
- Investigation: Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

As noted in figure 2, the three most prevalent types of incidents reported to US-CERT during fiscal years 2006 through 2008 were unauthorized access, improper usage, and investigation.

Figure 2: Percentage of Incidents Reported to US-CERT in FY06-FY08 by Category



Source: GAO analysis of US-CERT data.

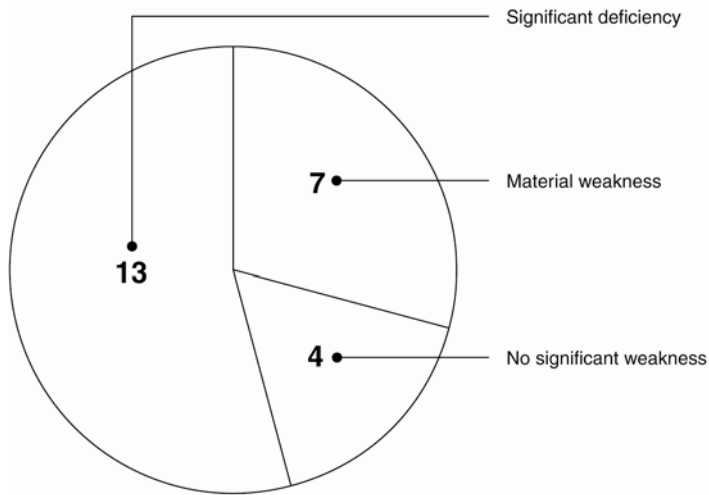
Vulnerabilities Pervade Federal Information Systems

The growing threats and increasing number of reported incidents, highlight the need for effective information security policies and practices. However, serious and widespread information security control deficiencies continue to place federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

In their fiscal year 2008 performance and accountability reports, 20 of 24 major agencies indicated that inadequate information system controls over financial systems and information were either a significant deficiency or a material weakness for financial statement reporting (see fig. 3).⁸

⁸A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

Figure 3: Number of Major Agencies Reporting Significant Deficiencies in Information Security



Source: GAO analysis of agency performance and accountability reports for FY2008.

Similarly, our audits have identified control deficiencies in both financial and nonfinancial systems, including vulnerabilities in critical federal systems. For example:

- We reported in September 2008⁹ that although the Los Alamos National Laboratory (LANL)—one of the nation’s weapons laboratories—implemented measures to enhance the information security of its unclassified network, vulnerabilities continued to exist in several critical areas, including (1) identifying and authenticating users of the network, (2) encrypting sensitive information, (3) monitoring and auditing compliance with security policies, (4) controlling and documenting changes to a computer system’s hardware and software, and (5) restricting physical access to computing resources. As a result, sensitive information on the network—including unclassified controlled nuclear information, naval nuclear propulsion information, export control information, and personally identifiable information—were exposed to an

⁹GAO, *Information Security: Actions Needed to Better Protect Los Alamos National Laboratory’s Unclassified Computer Network*, [GAO-08-1001](#) (Washington, D.C.: Sept. 9, 2008).

unnecessary risk of compromise. Moreover, the risk was heightened because about 300 (or 44 percent) of 688 foreign nationals who had access to the unclassified network as of May 2008 were from countries classified as sensitive by the Department of Energy, such as China, India, and Russia.

- In May 2008¹⁰ we reported that the Tennessee Valley Authority (TVA)— a federal corporation and the nation’s largest public power company that generates and transmits electricity using its 52 fossil, hydro, and nuclear power plants and transmission facilities—had not fully implemented appropriate security practices to secure the control systems used to operate its critical infrastructures. Both its corporate network infrastructure and control systems networks and devices at individual facilities and plants were vulnerable to disruption. In addition, the interconnections between TVA’s control system networks and its corporate network increased the risk that security weaknesses, on the corporate network could affect control systems networks and we determined that the control systems were at increased risk of unauthorized modification or disruption by both internal and external threats. These deficiencies placed TVA at increased and unnecessary risk of being unable to respond properly to a major disruption resulting from an intended or unintended cyber incident, which could then, in turn, affect the agency’s operations and its customers.

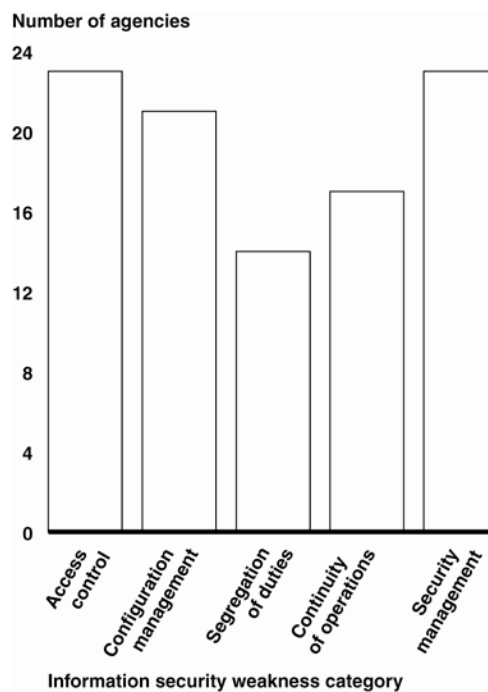
Weaknesses Persist in All Major Categories of Controls

Vulnerabilities in the form of inadequate information system controls have been found repeatedly in our prior reports as well as IG and agency reports. These weaknesses fall into five major categories of information system controls: (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) configuration management controls, which provide assurance that security features for hardware and software are identified and implemented and that changes to that configuration are systematically controlled; (3) segregation of duties, which

¹⁰GAO, *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks*, [GAO-08-526](#) (Washington, D.C.: May 21, 2008).

reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and (5) an agencywide information security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented. Figure 4 shows the number of major agencies with weaknesses in these five areas.

Figure 4: Number of Major Agencies Reporting Weaknesses by Control Category for Fiscal Year 2008



Source: GAO analysis of IG, agency, and prior GAO reports.

Over the last several years, most agencies have not implemented controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. Our analysis of IG, agency, and our own reports uncovered that agencies did not have adequate controls in place to ensure that only authorized individuals could access or manipulate data on their systems and networks. To illustrate, weaknesses were reported in such controls at 23 of 24 major agencies for fiscal year 2008. For example, agencies did not consistently (1) identify and authenticate users to prevent

unauthorized access, (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate, (3) establish sufficient boundary protection mechanisms, (4) apply encryption to protect sensitive data on networks and portable devices, and (5) log, audit, and monitor security-relevant events. At least nine agencies also lacked effective controls to restrict physical access to information assets. We previously reported that many of the data losses occurring at federal agencies over the past few years were a result of physical thefts or improper safeguarding of systems, including laptops and other portable devices.

In addition, agencies did not always configure network devices and services to prevent unauthorized access and ensure system integrity, patch key servers and workstations in a timely manner, or segregate incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction. Furthermore, agencies did not always ensure that continuity of operations plans contained all essential information necessary to restore services in a timely manner. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of information.

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements for an agencywide information security program. An agencywide security program, required by the Federal Information Security Management Act¹¹, provides a framework and continuing cycle of activity for assessing and managing risk, developing and implementing security policies and procedures, promoting security awareness and training, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. Our analysis determined that 23 of 24 major federal agencies had weaknesses in their agencywide information security programs.

¹¹*Federal Information Security Management Act of 2002, Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).*

Due to the persistent nature of these vulnerabilities and associated risks, we continued to designate information security as a governmentwide high-risk issue in our most recent biennial report to Congress;¹² a designation we have made in each report since 1997.

Opportunities Exist for Enhancing Federal Information Security

Over the past several years, we and the IGs have made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program shortfalls. For example, we recommended that agencies correct specific information security deficiencies related to user identification and authentication, authorization, boundary protections, cryptography, audit and monitoring, physical security, configuration management, segregation of duties, and contingency planning. We have also recommended that agencies fully implement comprehensive, agencywide information security programs by correcting shortcomings in risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions. The effective implementation of these recommendations will strengthen the security posture at these agencies.

In addition, the White House, the Office of Management and Budget (OMB), and certain federal agencies have continued or launched several governmentwide initiatives that are intended to enhance information security at federal agencies. These key initiatives are discussed below.

- *Comprehensive National Cybersecurity Initiative*: In January 2008, President Bush began to implement a series of initiatives aimed primarily at improving the Department of Homeland Security and other federal agencies' efforts to protect against intrusion attempts and anticipate future threats.¹³ While these initiatives have not been made public, the Director of National Intelligence stated that they

¹²GAO, *High-Risk Series: An Update*, [GAO-09-271](#) (Washington, D.C.: January 2009).

¹³The White House, National Security Presidential Directive 54/ Homeland Security Presidential Directive 23 (Washington, D.C.: Jan. 8, 2008).

include defensive, offensive, research and development, and counterintelligence efforts, as well as a project to improve public/private partnerships.¹⁴

- *The Information Systems Security Line of Business*: The goal of this initiative, led by OMB, is to improve the level of information systems security across government agencies and reduce costs by sharing common processes and functions for managing information systems security. Several agencies have been designated as service providers for IT security awareness training and FISMA reporting.
- *Federal Desktop Core Configuration*: For this initiative, OMB directed agencies that have Windows XP deployed and plan to upgrade to Windows Vista operating systems to adopt the security configurations developed by the National Institute of Standards and Technology, Department of Defense, and Department of Homeland Security. The goal of this initiative is to improve information security and reduce overall IT operating costs.
- *SmartBUY*: This program, led by the General Services Administration, is to support enterprise-level software management through the aggregate buying of commercial software governmentwide in an effort to achieve cost savings through volume discounts. The SmartBUY initiative was expanded to include commercial off-the-shelf encryption software and to permit all federal agencies to participate in the program. The initiative is to also include licenses for information assurance.
- *Trusted Internet Connections Initiative*: This is an effort designed to optimize individual agency network services into a common solution for the federal government. The initiative is to facilitate the reduction of external connections, including Internet points of presence, to a target of 50.

¹⁴Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

We currently have ongoing work that addresses the status, planning, and implementation efforts of several of these initiatives.

In summary, the threats to federal information systems are evolving and growing, and federal systems are not sufficiently protected to consistently thwart the threats. Unintended incidents and attacks from individuals and groups with malicious intent, such as criminals, terrorists, and adversarial foreign nations, have the potential to cause significant damage to the ability of agencies to effectively perform their missions, deliver services to constituents, and account for their resources. Opportunities exist to improve information security at federal agencies. The White House, OMB, and certain federal agencies have initiated efforts that are intended to strengthen the protection of federal information and information systems. Until such opportunities are seized and fully exploited, and agencies fully and effectively implement the hundreds of recommendations by us and by IGs to mitigate information security control deficiencies and implement agencywide information security programs, federal information and systems will remain vulnerable.

Chairwoman Watson, this concludes my statement. I would be happy to answer questions at the appropriate time.

Contact and Acknowledgments

If you have any questions regarding this report, please contact Gregory C. Wilshusen, Director, Information Security Issues, at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this report include Charles Vrabel (Assistant Director), Larry Crosland, Neil Doherty, Rebecca LaPaze, and Jayne Wilson.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

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

March 2010

CYBERSECURITY

Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative



GAO

Accountability * Integrity * Reliability



Highlights of [GAO-10-338](#), a report to congressional requesters

Why GAO Did This Study

In response to the ongoing threats to federal systems and operations posed by cyber attacks, President Bush established the Comprehensive National Cybersecurity Initiative (CNCI) in 2008. This initiative consists of a set of projects aimed at reducing vulnerabilities, protecting against intrusions, and anticipating future threats. GAO was asked to determine (1) what actions have been taken to develop interagency mechanisms to plan and coordinate CNCI activities and (2) what challenges CNCI faces in achieving its objectives related to securing federal information systems. To do this, GAO reviewed CNCI plans, policies, and other documentation and interviewed officials at the Office of Management and Budget (OMB), Department of Homeland Security, and the Office of the Director of National Intelligence (ODNI), among other agencies. GAO also reviewed studies examining aspects of federal cybersecurity and interviewed recognized cybersecurity experts.

What GAO Recommends

GAO is recommending that OMB take steps to address each of the identified challenges. OMB agreed with five of six recommendations, disagreeing with the recommendation regarding defining roles and responsibilities. However, such definitions are key to achieving CNCI's objective of securing federal systems.

View [GAO-10-338](#) or [key components](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshusen@gao.gov, or Davi D'Agostino at (202) 512-5431 or dagostinod@gao.gov.

CYBERSECURITY

Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative

What GAO Found

The White House and federal agencies have taken steps to plan and coordinate CNCI activities by establishing several interagency working groups. These include the National Cyber Study Group, which carried out initial brainstorming and information-gathering for the establishment of the initiative; the Communications Security and Cyber Policy Coordinating Committee, which presented final plans to the President and coordinated initial implementation activities; and the Joint Interagency Cyber Task Force, which serves as the focal point for monitoring and coordinating projects and enabling the participation of both intelligence-community and non-intelligence-community agencies. These groups have used a combination of status meetings and other reporting mechanisms to track implementation of projects.

CNCI faces several challenges in meeting its objectives:

- **Defining roles and responsibilities.** Federal agencies have overlapping and uncoordinated responsibilities for cybersecurity, and it is unclear where overall responsibility for coordination lies.
- **Establishing measures of effectiveness.** The initiative has not yet developed measures of the effectiveness in meeting its goals. While federal agencies have begun to develop effectiveness measures for information security, these have not been applied to the initiative.
- **Establishing an appropriate level of transparency.** Few of the elements of CNCI have been made public, and the rationale for classifying related information remains unclear, hindering coordination with private sector entities and accountability to the public.
- **Reaching agreement on the scope of educational efforts.** Stakeholders have yet to reach agreement on whether to address broad education and public awareness as part of the initiative, or remain focused on the federal cyber workforce.

Until these challenges are adequately addressed, there is a risk that CNCI will not fully achieve its goal to reduce vulnerabilities, protect against intrusions, and anticipate future threats against federal executive branch information systems.

The federal government also faces strategic challenges beyond the scope of CNCI in securing federal information systems:

- **Coordinating actions with international entities.** The federal government does not have a formal strategy for coordinating outreach to international partners for the purposes of standards setting, law enforcement, and information sharing.
- **Strategically addressing identity management and authentication.** Authenticating the identities of persons or systems seeking to access federal systems remains a significant governmentwide challenge. However, the federal government is still lacking a fully developed plan for implementation of identity management and authentication efforts.

Contents

Letter		1
	Conclusions	3
	Recommendations for Executive Action	4
	Agency Comments and Our Evaluation	5
Appendix I	Briefing to Congressional Staff on the Comprehensive National Cybersecurity Initiative	7
Appendix II	Comments from the Office of Management and Budget	55
Appendix III	Comments from the Office of the Director of National Intelligence	58
Appendix IV	GAO Contacts and Staff Acknowledgments	60

Abbreviations

CNCI	Comprehensive National Cybersecurity Initiative
HSPD	Homeland Security Presidential Directive
NCSC	National Cyber Security Center
NSPD	National Security Presidential Directive
OMB	Office of Management and Budget
ODNI	Office of the Director of National Intelligence
OSTP	Office of Science and Technology Policy
US-CERT	U.S. Computer Emergency Readiness Team

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

March 5, 2010

The Honorable Loretta Sanchez
Chairwoman
Subcommittee on Terrorism, Unconventional Threats and Capabilities
Committee on Armed Services
House of Representatives

The Honorable Adam Smith
House of Representatives

Pervasive and sustained cyber attacks against the United States continue to pose the threat of a potentially devastating impact on federal systems and operations. In January 2008, President Bush issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), establishing the Comprehensive National Cybersecurity Initiative (CNCI), a set of projects aimed at safeguarding executive branch information systems by reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats. Shortly after taking office, President Obama, in February 2009, ordered a review of cybersecurity-related plans, programs, and activities underway throughout the federal government, including the CNCI projects. This review resulted in a May 2009 report that made recommendations for achieving a more reliable, resilient, and trustworthy digital infrastructure.

We were asked to determine (1) what actions have been taken to develop interagency mechanisms to plan and coordinate CNCI activities and (2) what challenges CNCI faces in achieving its objectives related to securing federal information systems. To do this, we analyzed CNCI plans and related agency documentation and interviewed officials at the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), the Office of the Director of National Intelligence (ODNI), the Department of Justice, the Office of Science and Technology Policy (OSTP), the State Department, and the National Science Foundation. We also identified and reviewed recent studies, including GAO reports, that examined federal cybersecurity issues and interviewed agency officials and recognized cybersecurity experts.

On November 24, 2009, we briefed your staff on the results of our review. This report includes the materials used at the briefing, as well as the final

recommendations we are making to the Director of OMB. The full briefing materials, including details on our scope and methodology, are reprinted in appendix I.

We conducted this performance audit from December 2008 to March 2010 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.

In summary, we made the following major points in our original briefing in November 2009:

- The White House and federal agencies have established interagency groups to plan and coordinate CNCI activities. These include the National Cyber Study Group, the Communications Security and Cyber Policy Coordinating Committee, and the Joint Interagency Cyber Task Force. The groups have used status meetings and other reporting mechanisms to track implementation progress of CNCI projects.
- CNCI faces challenges in achieving its objectives related to securing federal information, which include reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats. These challenges include:
 - **Better defining agency roles and responsibilities.** Currently, agencies have overlapping and uncoordinated responsibilities for cybersecurity activities that have not been clarified by the initiative.
 - **Establishing measures of effectiveness.** Measures of the effectiveness of CNCI projects in increasing the cybersecurity of federal information systems have not been developed.
 - **Establishing an appropriate level of transparency.** Current classification of CNCI-related information may hinder the effectiveness of the initiative, particularly with respect to coordinating activities with the private sector and ensuring accountability to the public.
 - **Coordinating interactions with international entities.** None of the projects directly address the coordination of federal cybersecurity activities with international partners.

-
- **Strategically addressing identity management and authentication.** Homeland Security Presidential Directive 12 (HSPD-12) required a governmentwide standard for secure and reliable forms of identification. However, CNCI does not include any projects focused on enhancing identity authentication (i.e., the identification of people or systems attempting to access federal systems).
 - **Reaching agreement on the scope of education efforts.** Stakeholders have not yet reached agreement on the scope of cybersecurity education efforts.

As documented in the briefing, we obtained comments from OMB officials on a draft of the briefing itself, and, among other things, these officials raised concerns that not all of the challenges we identified were associated with specific CNCI projects. In subsequent discussions, these officials reiterated their concern that several of the challenges we identified involved matters that were beyond the scope of the CNCI's 12 projects. In response, we have clarified that two of the challenges we identified—coordinating actions with international entities, and strategically addressing identity management and authentication—are not connected to specific CNCI projects but rather relate to additional cybersecurity activities that are essential to securing federal systems, a key overall goal of CNCI.

In addition, OMB officials called our attention to an initial version of a plan for implementing federal identity, credential, and access management that was released in November 2009, when we presented our briefing. The plan, while not yet complete, is aimed at addressing the challenge we identified regarding identity management and authentication, and we have modified our conclusions and recommendation in this area to take into account this effort.

Conclusions

The White House and federal agencies have taken a number of actions to establish and use interagency mechanisms in planning and coordinating CNCI activities, and these groups have used status meetings and other reporting mechanisms to track the implementation progress of CNCI's component projects. Beginning with the work of the National Cyber Study Group in brainstorming and gathering information from multiple federal sources, the management approach for the initiative has emphasized coordination across agencies.

While planning for CNCI has been broadly coordinated, the initiative faces challenges if it is to fully achieve its objectives related to securing federal information systems, which include reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats. Among other things, roles and responsibilities for participating agencies have not always been clearly defined, and measures of effectiveness have not yet been established. These challenges have been highlighted by experts and in other recent reviews of federal cybersecurity strategies. Until they are addressed within CNCI, the initiative risks not fully meeting its objectives. While these issues relate directly to the projects that comprise CNCI, the federal government also faces strategic challenges in areas that are not the subject of existing projects within CNCI but remain key to achieving the initiative's overall goal of securing federal information systems. These challenges include coordination with international entities and the governmentwide implementation of identity management and authentication.

Recommendations for Executive Action

To address challenges that CNCI faces in achieving its objectives related to securing federal information systems, we are recommending that the Director of OMB take the following four actions:

- better define roles and responsibilities of all key CNCI participants, such as the National Cyber Security Center, to ensure that essential governmentwide cybersecurity activities are fully coordinated;
- establish measures to determine the effectiveness of CNCI projects in making federal information systems more secure and track progress against those measures;
- establish an appropriate level of transparency about CNCI by clarifying the rationale for classifying information, ensuring that as much information is made public as is appropriate, and providing justification for withholding information from the public; and
- reach agreement on the scope of CNCI's education projects to ensure that an adequate cadre of skilled personnel is developed to protect federal information systems.

To address strategic challenges in areas that are not the subject of existing projects within CNCI but remain key to achieving the initiative's overall goal of securing federal information systems, we are recommending that the Director of OMB take the following two actions:

-
- establish a coordinated approach for the federal government in conducting international outreach to address cybersecurity issues strategically; and
 - continue development of a strategic approach to identity management and authentication, linked to HSPD-12 implementation, as initially described in the Chief Information Officers Council’s plan for implementing federal identity, credential, and access management, so as to provide greater assurance that only authorized individuals and entities can gain access to federal information systems.

Agency Comments and Our Evaluation

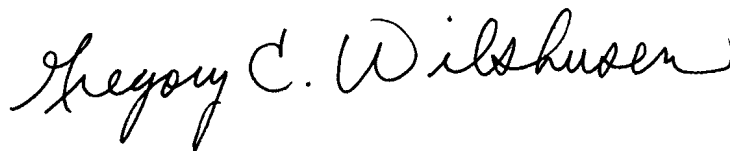
In written comments on a draft of this report, reproduced in appendix II, the Federal Chief Information Officer concurred with five of six recommendations, stating that efforts were either planned or underway to address them. OMB disagreed with our conclusions and recommendation regarding the need to better define roles and responsibilities of federal entities in securing federal systems, noting that specific agency roles and responsibilities for the CNCI initiatives had been clearly defined. We agree that, as described in our briefing, lead responsibility has been assigned for each of the CNCI initiatives. However, this fact does not diminish the larger challenge that CNCI faces in better establishing cybersecurity roles and responsibilities for securing federal systems. For example, as discussed in the briefing, the federal government’s response to the July 2009 attacks on its Web sites was not well-coordinated. Although OMB stated that such a response was not an activity specifically within CNCI, the poorly-coordinated response illustrates the larger challenge that CNCI faces in better establishing cybersecurity roles and responsibilities for securing federal systems.

Regarding the statement in the briefing that the National Cyber Security Center (NCSC) has not been fully operational and has had unclear responsibilities, OMB commented that NCSC’s responsibilities were distinct from those of other federal entities involved in incident detection and response. However, we disagree. For example, as discussed in the briefing, the United States Computer Emergency Readiness Team (US-CERT), which handles incident response, engages in extensive cross-agency coordination, and it remains unclear how this function differs from the responsibilities planned for NCSC. OMB also stated that it had requested that we clarify that the interagency policy committee is a formal mechanism for interagency coordination. In response to this comment, we previously changed wording in the draft briefing that had incorrectly implied that this committee was an informal mechanism.

The Director of Legislative Affairs of ODNI provided written comments on a draft of this report, which are reproduced in appendix III. In its comments, ODNI expressed concern that comments previously provided on the briefing slides remained largely unincorporated and requested that the report better reflect those comments. Specifically, in its earlier comments, ODNI had raised concern that CNCI should not be criticized for items that were not included in it. As previously discussed, to avoid potential misunderstanding, we have clarified that two of the challenges we identified are not connected to specific CNCI projects but rather relate to additional cybersecurity activities that are necessary to achieve CNCI's overall goal of securing federal information systems.

We are sending copies of this report to the Director of National Intelligence, the Director of the Office of Management and Budget, and to interested congressional committees. The report will also be available on the GAO Web site at no charge at <http://www.gao.gov>.

If you or your staff have any questions concerning this report, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Davi M. D'Agostino at (202) 512-5431 or dagostinod@gao.gov. Contact points for our Office of Congressional Relations and our Office of Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.



Gregory C. Wilshusen
Director, Information Security Issues



Davi M. D'Agostino
Director, Defense Capabilities and Management

Appendix I: Briefing to Congressional Staff on the Comprehensive National Cybersecurity Initiative



INFORMATION SECURITY: Progress and Challenges in Defining and Coordinating the Comprehensive National Cybersecurity Initiative

Briefing for Staff of the Subcommittee on Terrorism, Unconventional
Threats and Capabilities, House Armed Services Committee

November 24, 2009



Contents

Introduction

Objectives, Scope, and Methodology

Results in Brief

Background

Interagency Working Groups Were Established to Plan and Coordinate Comprehensive National Cybersecurity Initiative (CNCI) Activities

CNCI Faces Challenges in Achieving Its Objectives Related to Securing Federal Information Systems

Conclusions

Recommendations for Executive Action

Agency Comments and Our Evaluation

Attachment 1: Comments from the Office of the Director of National Intelligence (ODNI)



Introduction

Pervasive and sustained cyber attacks against the United States continue to pose the threat of a potentially devastating impact on federal systems and operations. In February 2009, the Director of National Intelligence testified that foreign nations and criminals had targeted government and private sector networks to gain a competitive advantage and potentially disrupt or destroy them, and that terrorist groups had expressed a desire to use cyber attacks as a means to target the United States. As recently as July 2009, press accounts reported that a widespread and coordinated attack over the course of several days targeted Web sites operated by major government agencies, including the Departments of Homeland Security and Defense, the Federal Aviation Administration, and the Federal Trade Commission, causing disruptions to the public availability of government information. Such attacks highlight the importance of developing a concerted response to safeguard federal systems.

In January 2008, President Bush issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), establishing the Comprehensive National Cybersecurity Initiative (CNCI), a set of projects with the objective of safeguarding federal executive branch government information systems by reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats.

In February 2009, President Obama directed the National Security and Homeland Security Advisors to conduct a review of the plans, programs, and activities underway throughout the government dedicated to cybersecurity, including the CNCI projects. The review resulted in a May 2009 report that recommended areas of action to help achieve a more reliable, resilient, and trustworthy digital infrastructure for the future.



Objectives, Scope, and Methodology

Our objectives were to determine

- (1) what actions have been taken to develop interagency mechanisms to plan and coordinate CNCI activities, and
- (2) what challenges CNCI faces in achieving its objectives related to securing federal information systems.

To determine what actions have been taken to develop interagency mechanisms to plan and coordinate CNCI activities, we analyzed CNCI plans and related agency documentation and interviewed responsible officials at the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), the Office of the Director of National Intelligence (ODNI), the Department of Justice, the Office of Science and Technology Policy (OSTP), the Department of State, and the National Science Foundation. Based on these sources, we compiled a chronology of actions taken related to the planning and coordination of CNCI.

To determine what challenges CNCI faces in achieving its objectives related to securing federal information systems, we identified and reviewed recent studies, including GAO reports, that examined federal cybersecurity issues at the same strategic level addressed by CNCI. We analyzed these studies to identify challenges directly applying to CNCI activities or relevant to the scope of CNCI and compared these with CNCI documentation and reported activities. We interviewed agency officials and recognized cybersecurity experts to confirm the identified challenges and obtain additional information.



Objectives, Scope, and Methodology

Our review did not include an assessment of the implementation of the Federal Information Security Management Act,¹ which provides a broad risk-based framework for managing federal information security activities.

We conducted this performance audit from December 2008 to November 2009 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.

¹Title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).



Interagency Working Groups Were Established to Plan and Coordinate CNCI Activities

The White House and federal agencies have established interagency groups to plan and coordinate CNCI activities. These groups have used a combination of status meetings and other reporting mechanisms to track implementation progress of CNCI's component projects. For example, agencies have been required to submit reports on progress and issues to an interagency task force, which has compiled the information into quarterly reports provided to the White House and OMB for use in monitoring the progress made by each of the CNCI projects.



CNCI Faces Challenges in Achieving Its Objectives Related to Securing Federal Information Systems

CNCI faces a number of key challenges in achieving its objectives related to securing federal information systems, which include reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats. These challenges include:

- *better defining agency roles and responsibilities*: Currently, agencies have overlapping and uncoordinated responsibilities for cybersecurity activities that have not been clarified in CNCI. CNCI is unlikely to achieve its goals until these roles are better clarified.
- *establishing measures of effectiveness*: Measures of the effectiveness of CNCI activities in increasing the cybersecurity of federal information systems have not yet been developed. Without such measures, the extent to which CNCI is achieving its goal of reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats is unclear.
- *balancing transparency with classification requirements*: Few elements of CNCI have been made public, and the rationale for how agencies classify information related to CNCI activities remains unclear. The lack of transparency regarding CNCI projects hinders accountability to Congress and the public. In addition, current classification may make it difficult for some agencies, as well as the private sector, to interact and contribute to the success of CNCI projects.



Results in Brief

- *coordinating interactions with international partners*: None of the 12 projects comprising CNCI directly address the coordination of international activities, which includes facilitating cooperation between cybersecurity and law enforcement professionals in different nations, developing security standards, and pursuing international agreements on engagement and information sharing. By addressing these issues in a coordinated way, CNCI could better achieve its objectives related to securing federal information systems.
- *strategically addressing identity management and authentication*: The federal government has long been challenged in employing effective identity management and authentication technologies; however, CNCI does not include an effort strategically focused on enhancing identity authentication across the federal government. CNCI is unlikely to be fully successful without addressing identity management and authentication.
- *reaching agreement on the scope of education efforts*: CNCI stakeholders have not yet reached agreement on whether the initiative should focus strictly on training the current workforce or include K-12, college, and graduate-level programs. Until agreement is reached, cybersecurity education will not be fully addressed by CNCI.

We are recommending that the Director of National Intelligence and the Director of the Office of Management and Budget take steps to address these challenges within CNCI.



Results in Brief

We provided a draft of this briefing to OMB, ODNI, and the Department of State for review and comment. In comments provided via e-mail, OMB stated that it agreed that many areas of federal cybersecurity could use improvement but disagreed that these issues are all related to CNCI. Similarly, ODNI agreed that the challenges we identified should have been included or accounted for in CNCI but raised concern that the program should not be criticized for items that were not included in it. We agree that CNCI was not intended to subsume all activities related to cybersecurity and have clarified our briefing to avoid a potential misunderstanding. Nevertheless, we believe that the challenges we identified remain of critical importance in determining whether CNCI can achieve its objectives related to securing federal information systems. The State Department did not indicate whether it agreed or disagreed with the content of the briefing. OMB, ODNI, and State also provided technical comments that we have addressed as appropriate in the final briefing.



Background

In January 2008, the President issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), establishing the Comprehensive National Cybersecurity Initiative (CNCI), a set of projects designed to safeguard federal government information systems by reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats.

According to the Department of Homeland Security (DHS), the three overall goals of CNCI are to

- establish a frontline defense—reduce current vulnerabilities and prevent intrusions;
- defend against the full spectrum of threats by using intelligence and strengthening supply chain security; and
- shape the future environment by enhancing research, development, and education as well as investing in leap-ahead technologies.



Background

NSPD-54/HSPD-23 established 12 CNCI projects and identified lead agencies for each.² Since January 2008, the lead agencies have been responsible for tracking progress on each of the projects specified in the directive.

Four agencies have responsibilities for multiple projects of CNCI:

- DHS's responsibilities focus on protecting civilian agency information systems, including reducing and consolidating external access points, deploying passive network sensors, and defining public and private partnerships.
- The Department of Defense (DOD) is charged with monitoring military information systems, increasing the security of classified networks, and deploying intrusion prevention systems, among other things.
- ODNI is responsible for monitoring intelligence community information systems and other intelligence-related activities, including the development of a governmentwide cyber counterintelligence plan.
- OSTP, which is responsible for providing advice on the effects of science and technology on domestic and international affairs, is responsible for the two CNCI projects that focus on advanced technology research and development.

OMB, the Department of Justice, and the National Security Council also have lead roles on specific CNCI projects.

²With the exception of DHS, budget data for CNCI projects is classified. In fiscal year 2009, \$254.9 million was appropriated for DHS activities related to CNCI efforts. According to DHS officials, the President's fiscal year 2010 budget proposed \$334 million to support CNCI at DHS.



Background

Table 1 lists and describes all 12 projects, and identifies the lead agency or agencies responsible for each.

Table 1: CNCI Projects and Lead Agencies

Project	Description	Lead agency/agencies
Trusted Internet Connections	Reduce and consolidate external access points with the goal of limiting points of access to the Internet for executive branch civilian agencies	OMB / DHS
Einstein 2	Deploy passive sensors across executive branch civilian systems that have the ability to scan the content of Internet packets to determine whether they contain malicious code	DHS
Einstein 3	Pursue deployment of intrusion prevention system that will allow for real-time prevention capabilities that will assess and block harmful code	DHS / DOD
Research and Development Efforts	Coordinate and redirect research and development (R&D) efforts with a focus on coordinating both classified and unclassified R&D for cybersecurity	OSTP
Connecting the Centers (includes National Cyber Security Center)	Connect current cyber centers to enhance cyber situational awareness and lead to greater integration and understanding of the cyber threat	ODNI

**Appendix I: Briefing to Congressional Staff on
the Comprehensive National Cybersecurity
Initiative**



Background

Project	Description	Lead agency/agencies
Cyber Counterintelligence Plan	Develop governmentwide cyber counterintelligence plan by improving the security of the physical and electromagnetic integrity of U.S. networks	ODNI / Department of Justice
Security of Classified Networks	Increase the security of classified networks to reduce the risk of information contained on the government's classified networks being disclosed	DOD / ODNI
Expand Education	Expand education efforts by constructing a comprehensive federal cyber education and training program, with attention to offensive and defensive skills and capabilities	DHS / DOD
Leap-Ahead Technology	Define and develop enduring leap-ahead technology, strategies, and programs by investing in high-risk, high-reward research and development and by working with both private sector and international partners	OSTP
Deterrence Strategies and Programs	Define and develop enduring deterrence strategies and programs that focus on reducing vulnerabilities and deter interference and attack in cyberspace	National Security Council
Global Supply Chain Risk Management	Develop multi-pronged approach for global supply chain risk management while seeking to better manage the federal government's global supply chain	DHS / DOD
Public and Private Partnerships "Project 12"	Define the federal role for extending cyber security into critical infrastructure domains and seek to define new mechanisms for the federal government and industry to work together to protect the nation's critical infrastructure	DHS

Source: GAO analysis of DHS and publicly available information.



Background

Several studies and expert groups have presented findings and recommendations that relate to the progress and comprehensiveness of CNCI. For example, in December 2008, the Center for Strategic and International Studies (CSIS), a bipartisan, nonprofit research and analysis organization, released a report by its Commission on Cybersecurity for the 44th Presidency which noted that although the CNCI was a good start, it was not sufficient to address the urgent national security problem of protecting cyberspace. The report concluded that the new administration should adopt the efforts of CNCI and work toward a comprehensive approach to cybersecurity.

Similarly, in March 2009 we reported on panel discussions we held with experts on critical aspects of the nation's cybersecurity strategy, including areas for improvement.³ The experts, who included former federal officials, academics, and private sector executives, highlighted key improvements that were, in their view, essential to updating the strategy and our national cybersecurity posture. Improvements they identified include developing a national strategy that clearly articulates strategic objectives, goals, and priorities and establishing a governance structure for implementing the strategy.

³GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, GAO-09-432T (Washington, D.C.: March 10, 2009).



Background

In May 2009, the President announced the results of a policy review of the plans, programs, and activities underway throughout the government dedicated to cybersecurity, including CNCI. The report recommended that CNCI activities be evaluated as one near-term action to help achieve a more reliable, resilient, and trustworthy digital infrastructure for the future.

As the policy review recommended, the President established a cybersecurity coordinator position to, among other things, integrate the government's cybersecurity policies. The policy review recommended that the coordinator perform the following actions related to CNCI:

- **Revise the nation's cyber strategy.** The review recommended that the cybersecurity coordinator prepare an updated national strategy to secure the information and communications infrastructure, including a continued evaluation of CNCI activities. The review recommended that consideration be given to the need for adjustments or additions to CNCI implementation plans.
- **Consider options for monitoring and coordination responsibilities.** The review noted that various oversight functions for cybersecurity efforts were performed outside of the Executive Office of the President. During the course of the review, a variety of structural options were suggested for the cybersecurity coordinator to coordinate and oversee cybersecurity activities, several of which would establish oversight responsibilities for CNCI within OMB or the Executive Office of the President.

These actions have not yet been implemented.



Interagency Coordination Mechanisms
National Cyber Study Group

Interagency Working Groups Were Established to Plan and Coordinate CNCI Activities

The White House and key agencies took several actions to develop interagency mechanisms to plan and coordinate the proposed projects that would be grouped together as the CNCI. Existing interagency working groups were used and new ones established to develop and coordinate the planned projects. Specific groups used or established in connection with development of CNCI included:

- **National Cyber Study Group (NCSG).** The NCSG was the original interagency group that was convened to do brainstorming and information-gathering as preparation for establishment of CNCI, according to key agency officials involved in the group. In May 2007, the President directed the Director of National Intelligence to conduct a review of the federal government's cybersecurity status. In response, the Director established the NCSG, composed of senior executives from over 20 agencies, led by ODNI. During the course of its work, the NCSG gathered information about major civilian, defense, and intelligence agencies to understand their roles and responsibilities in federal cybersecurity efforts. The NCSG met twice a week for several months to understand agencies' roles in national cybersecurity, their capabilities, and the overall threats to federal networks.



Interagency Coordination Mechanisms
Policy Coordinating Committee

• **Communications Security and Cyber Policy Coordinating Committee (PCC).** The PCC, a White House coordinating committee, was the chief mechanism used for presenting final CNCI plans to the President and coordinating initial implementation actions after the program was approved, according to key agency officials involved with the group.⁴ In late 2007, the NCSG transferred its initial planning work on CNCI to the PCC, which was co-chaired by the Homeland Security Council (HSC) and the National Security Council (NSC), and had been in existence prior to taking on the CNCI task. Six sub-groups of the PCC were established as focal points for specific issues to support the work of the larger committee.

Shortly after the transfer from NCSG, the PCC presented its CNCI proposal to the President. The proposal included a set of cybersecurity projects that would make up the initiative. The White House used this as the basis for NSPD-54/HSPD-23, which was approved by the President in January 2008.

The PCC immediately began overseeing CNCI implementation. According to an OMB official, in the 12 months following the approval of NSPD-54/HSPD-23, the PCC met weekly to assess CNCI projects' performance. Once a quarter, a meeting was held to conduct a more in-depth review of the projects.

⁴Following the change in administration in 2009, the PCC was re-named the Information and Communications Infrastructure Interagency Policy Committee (ICI IPC).



Interagency Coordination Mechanisms Joint Interagency Cyber Task Force

• **Joint Interagency Cyber Task Force.** According to ODNI, NSPD-54/HSPD-23 assigned it the responsibility to monitor and coordinate the implementation of CNCI, and to do so in coordination with the Secretaries of State, the Treasury, Defense, Commerce, Energy, and Homeland Security, and the Attorney General.

To address these responsibilities, ODNI established a Joint Interagency Cyber Task Force (JIACTF) in February 2008. The mission of the task force was to serve as the focal point for monitoring and coordinating the CNCI projects and to enable the participation of both Intelligence Community (IC) and non-IC agencies in the overall CNCI effort. Its responsibilities included establishing performance measures for monitoring implementation of the initiative.

According to the acting director of the JIACTF, although ODNI served as a coordinator through the task force, it was not authorized to direct other agencies to complete CNCI tasks. The acting director stated that ODNI is only responsible for monitoring and reporting to the President on CNCI activities.



Interagency Coordination Mechanisms Interagency Working Groups

The JIACTF and PCC used a combination of status meetings and other reporting mechanisms to track implementation progress of the CNCI's component projects:

- **Interagency Working Groups.** For each of the CNCI projects, interagency working groups developed specific deliverables called for by the presidential directive, such as implementation plans and other reports.

According to ODNI, the JIACTF assisted each working group in drafting 3-, 9-, 18-, and 36-month target implementation goals, against which their progress was to be measured by the JIACTF.⁵ According to ODNI, the measures were established to ensure that CNCI deliverables were being submitted in a timely manner and that the White House was aware of when actions were due or of unresolved issues. ODNI reported that over 80 measures were being tracked.

⁵ODNI noted that implementation goals were also included for 12-, 24-, and 30-month activities for some initiatives.



Interagency Coordination Mechanisms Quarterly Reports

- **Quarterly Reports.** Agencies were required to submit reports on progress and issues to the JIACTF, which compiled aggregate reports based on these submissions. According to ODNI, the task force conducted follow-up meetings with agency leads to address any outstanding issues. In addition, it met quarterly with CNCI project leads to conduct in-depth discussions of successes, remaining challenges, and risks.

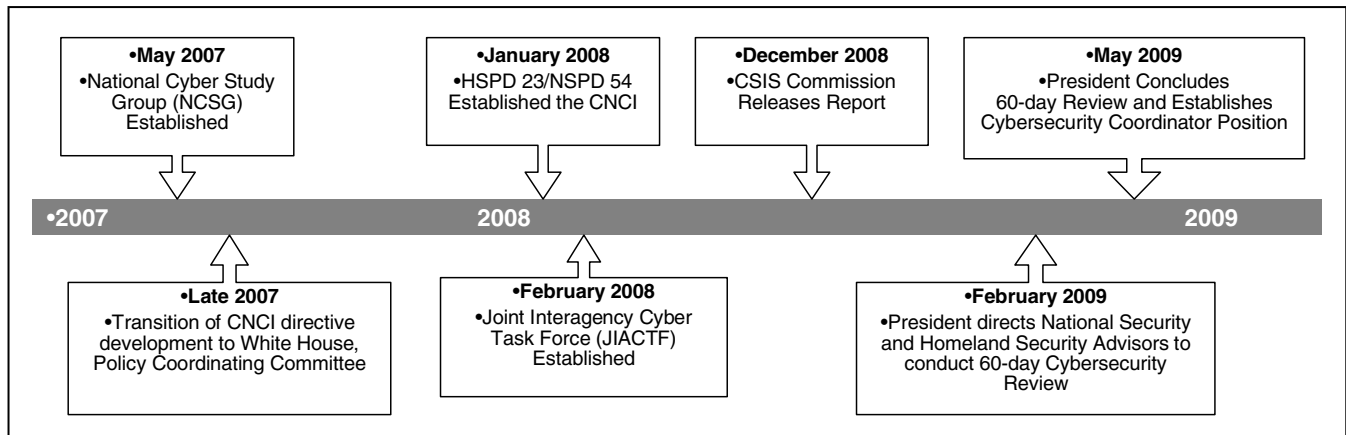
On a quarterly basis, the task force submitted reports to the White House, with copies provided to OMB, outlining the status of CNCI and offering recommendations. The reports indicated which activities were on schedule or needed further attention by JIACTF members. According to ODNI, these reports reflected discussions with agency leads and focused on target achievements, recent accomplishments, planned activities and schedules, challenges, risks and mitigation strategies, information on budget and staffing, performance measures, critical issues, and recommendations. An OMB official stated that the content of these reports became more detailed over time.



Interagency Coordination Mechanisms

The following figure summarizes key actions to develop interagency mechanisms for coordinating CNCI in the context of other related cybersecurity events.

Figure 1: Timeline of Actions to Develop Interagency Mechanisms and Other CNCI-Related Events



Source: GAO analysis of agency data.



CNCI Faces Challenges Roles and Responsibilities

CNCI Faces Challenges in Achieving its Objectives Related to Securing Federal Information Systems

CNCI faces a number of key challenges in achieving its objectives related to securing federal information systems, which include reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats.

Better Defining Agency Roles and Responsibilities

We previously reported that clearly defining areas of responsibility is a key internal control that provides management with a framework for planning, directing, and controlling operations to achieve goals.⁶ To collaborate effectively, agencies need to define and agree on their respective roles and responsibilities, including how the collaborative effort will be led. Doing so can help to organize joint and individual efforts and facilitate decision-making.⁷ Commitment by those involved in the collaborative effort, from all levels of the organization, is also critical to overcoming the many barriers to working across agency boundaries. Clearly defining roles and responsibilities in securing federal information systems is particularly important because such systems are highly interconnected, and their security is a critical element of the nation's overall security.

⁶GAO, *Internal Control: Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

⁷GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: October 21, 2005).



CNCI Faces Challenges Roles and Responsibilities

Currently, agencies have overlapping and uncoordinated responsibilities for cybersecurity activities that have not been clarified by CNCI. A key example is the lack of agreement regarding which agency is responsible for leading efforts in cyber information sharing and situational awareness. Specifically, NSPD-54/HSPD-23 directed the Secretary of Homeland Security to establish a National Cyber Security Center (NCSC) to coordinate and integrate information to secure networks and systems. However, several other cybersecurity response centers—including one within DHS—have many of the same responsibilities as NCSC for coordinating the federal response to cybersecurity incidents. According to the then-acting director of the NCSC, due to a lack of coordination among the top level of agencies and the White House, the center has not been fully operational, and it was unclear what responsibilities it was to assume for the federal government as a whole.

Further, the Secretary of Homeland Security recently stated that DHS was not sufficiently organized to achieve the goals of interagency cybersecurity programs, which include CNCI projects at DHS. The Secretary stated that all cyber responsibilities at DHS were moved under the Deputy Under Secretary for National Protection and Programs in June to address this issue. However, the acting director of the NCSC noted that the NCSC remains separate from other DHS cybersecurity programs and is still not fully operational. Specifically, she stated that although the NCSC is now funded through the National Protection and Programs Directorate, it continues to report independently to the Secretary of Homeland Security.



CNCI Faces Challenges Roles and Responsibilities

Another example of overlapping and uncoordinated responsibilities is federal agencies' response to the July 2009 cyber attacks on U.S. government Web sites. The Acting White House Cybersecurity Policy Advisor noted that agencies had responded in an ad hoc manner to these attacks and that the response had not been well-coordinated. She added that to establish specific roles, functions, and relationships among federal government security personnel in responding to an incident, DHS plans to develop a national incident response plan by the end of 2009.

While not addressing the specifics of CNCI project roles and responsibilities, experts have discussed the broader challenge of overlapping roles and responsibilities regarding federal cybersecurity, which has an impact on achieving CNCI objectives. For example:

- The CSIS commission stated that the central problems in the current federal organization for cybersecurity are lack of a strategic focus, overlapping missions, poor coordination and collaboration, and diffuse responsibility. To combat these challenges, the commission recommended the creation of a new cyberspace office in the Executive Office of the President that could leverage the knowledge of resources across federal agencies in order to provide the best security for our nation.
- Our expert panel raised concerns about how national security agencies coordinate with law enforcement agencies on issues of cybersecurity. Specifically, they stated that national security agencies often times overlooked the value and resources that law enforcement agencies had to offer on cybersecurity issues.



CNCI Faces Challenges Roles and Responsibilities

- The White House policy review stated that the federal government is not organized to effectively address cybersecurity challenges. Specifically, it stated that responsibilities for cybersecurity are distributed across a wide array of federal agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that allow for consistency in dealing with often-conflicting issues. The policy review recommended that the President's new cybersecurity policy official work with agencies to recommend coherent, unified policy guidance where necessary to clarify authorities, roles, and responsibilities for cybersecurity-related activities across the federal government.

CNCI is unlikely to fully achieve its goal of reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats to federal information systems unless roles and responsibilities for cybersecurity activities across the federal government are more clearly defined and coordinated.



CNCI Faces Challenges Effectiveness Metrics

Establishing Measures of Effectiveness

As we previously reported, measuring performance allows organizations to track the progress they are making toward their goals and gives managers crucial information on which to base their organizational and management decisions.⁸ For example, performance metrics are valuable to management when forecasting future budgetary needs. Leading organizations also recognize that performance measures can create powerful incentives to influence organizational and individual behavior. Additionally, when appropriate, making performance measurements available to the public demonstrates transparency, allowing the public to see evidence of program effectiveness.

Measures of the effectiveness of CNCI activities in increasing the cybersecurity of federal information systems have not yet been developed. Although CNCI plans contain milestones for tracking implementation progress (such as the timely submission of development deliverables), they do not have corresponding benchmarks for effectiveness to gauge the extent to which CNCI activities are improving cybersecurity.

⁸GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, GAO/GGD-96-118 (Washington, D.C.: June 1996).



CNCI Faces Challenges Effectiveness Metrics

While two of the CNCI implementation plans we reviewed outlined future efforts to establish performance measures to assess progress towards achieving the initiatives' goals, other plans did not include such measures. Specifically, the Research and Development Coordination and Leap-Ahead Technologies initiatives planned to set measures for, among other things, quality of research, direct impact (where research results are adopted for operational use), and indirect impact (such as developing new collaborations or technology transfer agreements). Other CNCI projects had not defined measures such as these. OMB stated that it intends to develop effectiveness metrics once the implementation stages of the projects are finished.

The federal government has recently begun taking action to develop effectiveness metrics for information security, and the results of these efforts may be applicable to CNCI. For example, recently, the federal CIO Council—the principal interagency forum for federal chief information officers—began efforts to promote the development and use of standard performance metrics that measure improvements in agencies' security posture over time and ensure that collaborative federal cybersecurity capabilities are prioritized. In addition, OMB has begun assembling a working group of federal agencies, advisory groups, and private sector partners to develop information security metrics that give insight into agencies' security postures on an on-going basis. OMB plans to release its new metrics by February 2010. While these efforts could assist CNCI implementation by developing effectiveness measures for use across the federal government, neither is currently part of CNCI.



CNCI Faces Challenges Effectiveness Metrics

The importance of measuring the effectiveness of cybersecurity programs has been underscored in recent assessments:

- The CSIS commission stated that a central part of judging whether a product or initiative has improved security is to develop metrics that can measure progress. However, the commission added that the federal government lacks meaningful measures of security. In addition, the commission stated that agencies should place greater emphasis on the periodic testing of information security procedures, policies, and practices required by the Federal Information Security Management Act of 2002 (FISMA). It added that agencies could use “red-team” attack assessments and recorded outcomes, in addition to the FISMA testing, as inputs to their effectiveness metrics.⁹
- The recent White House policy review stated the need for cybersecurity programs to have a defined purpose and metrics to evaluate whether their goals are achieved. Specifically, within its near-time action plan, it recommended designating cybersecurity as one of the President’s key management priorities and establishing performance metrics.

⁹“Red team” simulated network attack exercises are used as a way to test responsiveness and evaluate different aspects of an agency’s overall security posture. Recorded outcomes of activities as a result of the simulation—such as the amount of time it takes for a password, network, or server to be compromised—can be used by management to prioritize projects aimed at reducing cyber attack risks.



CNCI Faces Challenges Effectiveness Metrics

- In September 2009, we reported on the current shortcomings of performance metrics for evaluating federal agencies' information security controls and programs.¹⁰ Specifically, we reported that federal agencies had tended to rely on measures of compliance with legal requirements, internal policies, or industry standards. We noted that until OMB revises its reporting guidance to require a more balanced range of measures and adherence to key practices in developing those measures, agencies are likely to continue to predominantly rely on measures that are of only limited value in assessing the effectiveness of their information security programs.

Without mechanisms to measure the effectiveness of federal cybersecurity efforts, the extent to which CNCI is achieving its goal of reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats is unclear. Particularly for agencies with multiple cyber responsibilities, both inside and outside of CNCI, effectiveness metrics would assist with prioritizing projects to get the best results. Establishing such measures would, as appropriate, allow federal officials, Congress, and the public to determine how effective CNCI projects and other cybersecurity efforts are at making federal information systems more secure.

¹⁰GAO, *Information Security: Concerted Effort Needed to Improve Federal Performance Measures*, GAO-09-617 (Washington, D.C.: September 14, 2009).



CNCI Faces Challenges Transparency

Establishing an Appropriate Level of Transparency

We previously reported that transparency is essential to improving government performance, ensuring accountability, and maintaining public trust. An appropriate level of transparency requires finding the right balance between restricting access to sensitive information and making such information available to Congress, other government agencies, private sector and international partners, and the public.¹¹ In January 2009, the President issued a memorandum to the heads of executive departments and agencies, committing them to greater transparency to promote accountability and provide information for citizens about what their government is doing.

Since the approval of NSPD-54/HSPD-23, few elements of CNCI have been made public. For example, agency press releases and statements by government officials have provided limited information regarding CNCI and its component projects. In addition, while OMB released guidance on the implementation of the governmentwide Trusted Internet Connections project, which aims to reduce connection points between agencies and the Internet, few details have been publicly released for other projects, such as Einstein 3 and Deterrence Strategies and Programs. The Einstein 3 project, which aims to prevent intrusion into federal networks by scrutinizing Internet traffic, has raised privacy concerns, but DHS has yet to release documentation of Einstein 3's privacy protection mechanisms.

¹¹GAO, *Transparent Government and Access to Information: A Role for Supreme Audit Institutions*, GAO-07-1068CG (Washington, D.C.: June 26, 2007).



CNCI Faces Challenges Transparency

Further, NSPD-54/HSPD-23 itself was written at a classified level and remains so. Officials from the Department of State and the National Cyber Security Center stated that the classification level of the directive hindered their ability to work with outside organizations. They added that the JIACTF and White House are planning to review the directive and CNCI projects to determine whether portions should be declassified.

The rationale for how agencies classify information related to CNCI activities remains unclear. For example, the supply chain risk management program presumably engages the private sector, but is entirely classified at the Secret level and higher. While DHS officials stated that a CNCI classification guide had been developed by ODNI, they did not provide a copy. DHS officials were also unable to provide justification for decisions made about which aspects of the initiative to make public.

Since CNCI's inception, former and current government officials have voiced concerns regarding the lack of publicly available information. For example:

- The federally-chartered Information Security and Privacy Advisory Board (ISPAB) stated that greater clarity and transparency was necessary to ensure both the effectiveness and trustworthiness of CNCI. Specifically, the ISPAB advised that government agencies release key documentation regarding the impact of CNCI activities on personal privacy.



CNCI Faces Challenges Transparency

- The CSIS commission noted that because the CNCI directive and projects are classified, little information could be shared with the public, the cybersecurity industry, or allied nations. The commission concluded that greater openness is important given the large role played by those outside the federal government in cybersecurity. In addition, the commission stated that the United States should open the discussion of how best to secure cyberspace and present the issues of deterrence and national strategy to the broad national community of experts and stakeholders.
- The White House policy review stated that, in moving forward, transparency would be important to build trust between the public and federal cybersecurity programs. The review added that it would be important to bring transparency and effective management to the overall cybersecurity portfolio.

While certain aspects and details of CNCI must necessarily remain classified, the lack of transparency regarding CNCI projects hinders accountability to Congress and the public. In addition, current classification may make it difficult for some agencies, as well as the private sector, to interact and contribute to the success of CNCI projects.



CNCI Faces Challenges
International Outreach

Coordinating Interactions with International Entities

Federal information systems operate in a cyberspace that is affected by individuals and nations from all over the world. Effective federal cybersecurity requires coordinated interaction with other nations. For example:

- *Pursuing law enforcement investigations and prosecutions* – Criminals operating in cyberspace can route their attacks through multiple computers located in different nations. As law enforcement officials trace such illegal activities across national boundaries, they must work with officials from those nations for permission and assistance in continuing the investigations. According to FBI officials, in order to pursue investigations quickly and efficiently, cybersecurity and law enforcement professionals must have agreements in place that facilitate cooperation.
- *Developing security standards for the Internet* – Communications and transactions in cyberspace occur over a common, global infrastructure (the Internet). Federal information systems connect to the Internet to communicate with contractor systems, the public, and other agency systems. Major decisions regarding the technical aspects of the Internet, such as security elements within common protocols and management of the Internet are increasingly being debated at an international level. The Acting White House Cybersecurity Policy Advisor has stated that to ensure that federal requirements are taken into account in these discussions, the federal government needs to carefully coordinate its participation.



CNCI Faces Challenges International Outreach

- *Defining rules of engagement* – The severity of recent cyber incidents has raised questions about the types of actions government agencies may take to defend themselves from attack. For example, agency officials may wish to disable a computer attacking from another nation in order to stop the attack. Further, acceptable behavior for engaging attackers in cyberspace may evolve as new technologies and types of attacks are created. In this regard, as the CSIS commission has pointed out, establishing a coordinated process for proposing and refining rules of engagement and negotiating related agreements with foreign governments is of critical importance.
- *Sharing information for situational awareness* – Exchanging information about recent attacks with other nations is critical for cybersecurity professionals to understand vulnerabilities, attack methods, and other current and emerging trends. According to the White House policy review, it is also necessary for coordinating responses to international cyber incidents.

The coordination of federal cybersecurity activities with international entities was not included within the scope of CNCI. Various agencies have independent efforts underway to address international cybersecurity issues. However, none of the 12 CNCI projects directly address the coordination of international activities.



CNCI Faces Challenges International Outreach

The federal government has not fully resolved issues regarding how to coordinate international cybersecurity activities. For example, according to FBI officials, federal agencies have relied on relationships that they have established individually with international partners to share information regarding law enforcement investigations. The officials stated that a formal interagency mechanism had not yet been developed to coordinate engagement with international partners on such investigations.

According to Department of State and FBI officials, a sub-group of the White House interagency policy committee that oversees CNCI projects acts as a forum for the coordination of international cybersecurity activities. However, the group has not developed a formal strategy for coordinating international outreach.

Experts have also identified international outreach on cybersecurity issues as a major challenge to the federal government. For example:

- The CSIS commission noted that the international aspects of cybersecurity have been among the least developed elements of U.S. cybersecurity policy. The commission added that CNCI is lacking in efforts to coordinate with international partners.
- Our panel of cybersecurity experts stated that greater attention must be focused on addressing the global aspects of cyberspace, including developing treaties, establishing standards, and pursuing international agreements. For example, panel members stated that the U.S. should pursue a more coordinated, aggressive approach.



CNCI Faces Challenges
International Outreach

- The White House policy review reiterated the need for a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards, acceptable legal norms, sovereign responsibility, and the use of force. For example, the policy review pointed out that the Council of Europe Convention on Cybercrime was an important international effort to achieve consistency in cybercrime laws and law enforcement efforts that had yet to be endorsed by many nations.

Addressing international efforts includes improving cooperation between cybersecurity and law enforcement professionals in different nations, developing security standards, and pursuing international agreements on engagement and information sharing. By addressing these issues in a coordinated way, CNCI could better achieve its objectives related to securing federal information systems.



CNCI Faces Challenges Identity Management and Authentication

Strategically Addressing Identity Management and Authentication

Confirming the identity of people and systems attempting to access federal networks is an essential step in ensuring the security of those information systems. As we previously reported, this confirmation process, known as authentication, provides assurance that only authorized individuals and other entities can gain appropriate access to federal information systems. Authentication and identity management use a variety of technologies, including passwords, electronic identification cards, and biometric identifiers, to provide different levels of assurance based on the sensitivity of the data being protected.¹²

The federal government has long been challenged in employing effective identity management and authentication technologies. For example, in an effort to increase the quality and security of federal identification and credentialing practices, the President issued Homeland Security Presidential Directive 12 (HSPD-12) in August 2004, requiring the establishment of a governmentwide standard for secure and reliable forms of identification. However, as we have previously reported, agencies have struggled to implement the authentication requirements of HSPD-12.¹³ For example, most agencies had not made full use of the electronic authentication capabilities available on the personal identification verification cards that they had issued or had plans to do so.

¹²GAO, *Electronic Government: Additional OMB Leadership Needed to Optimize Use of New Federal Employee Identification Cards*, GAO-08-292 (Washington, D.C.: February 29, 2008).

¹³GAO-08-292.



CNCI Faces Challenges Identity Management and Authentication

CNCI does not include any projects focused on enhancing identity authentication. Instead, its operational projects are dedicated to areas such as intrusion detection and prevention, limiting the number of Internet nodes, and deterrence strategies. While these are important, there is no strategic effort to address the issue of authenticating users appropriately and consistently across federal systems and networks.

Cybersecurity experts have reaffirmed the need for identity management and authentication across the federal government. For example:

- The National Science and Technology Council—the principal group within the White House to coordinate policy among federal research and development agencies—reported in 2008 on major deficiencies in federal identity management efforts.¹⁴ The council concluded that the federal government is only beginning to work toward a consistent approach to identity management, and that there is no single organization responsible for coordinating governmentwide identity management.

¹⁴The National Science and Technology Council, *Identity Management Task Force Report 2008* (Washington D.C., 2008).



CNCI Faces Challenges Identity Management and Authentication

- According to the CSIS commission, strong authentication significantly improves defensive capabilities, but the federal government has not succeeded in improving authentication, and it is not addressed by the CNCI directive. The commission recommended that the President require agencies to report on the status of their compliance with HSPD-12 and restrict bonuses and awards at agencies that have not fully complied with the implementation of the directive.
- The White House policy review stated that cybersecurity cannot be improved without improving authentication. Specifically, it stated that the federal government—in collaboration with industry and the civil liberties and privacy communities—should build a cybersecurity-based identity management vision and strategy for the nation that considers an array of approaches, including privacy-enhancing technologies. It further stated that the federal government should ensure resources are available for full federal implementation of HSPD-12. In July 2009, the Acting White House Cybersecurity Policy Advisor stated that work had begun on a framework to set priorities in the area of identity management.

Using strong methods of identifying people and systems attempting to access federal systems and sensitive information is an essential part of a comprehensive security program to strengthen cybersecurity. Without a strategic approach to enhancing identity management and authentication linked to HSPD-12 implementation, CNCI is unlikely to be fully successful in addressing the security of the federal government's information systems and assets.



CNCI Faces Challenges Scope of Education Efforts

Reaching Agreement on the Scope of Education Efforts

Training and education within the federal government are key for ensuring that safe and secure practices are exercised by federal employees when they access government information systems. In addition, our panel of cybersecurity experts stated that the federal government should raise public awareness about the seriousness of cybersecurity issues and that many national leaders in business and government are generally not aware of the severity of the risks to national and economic security posed by cybersecurity threats. Further, in order to maintain the security of federal information systems, agencies need properly trained cybersecurity professionals.

DHS's cybersecurity education efforts currently focus on the training and education of the current and future federal workforce. According to the lead DHS official for cybersecurity education, the CNCI directive requires DHS and DOD to develop a strategy and recommendations for prioritizing and redirecting current educational efforts to build a skilled cyber workforce and ensuring the development of skilled individuals for future federal government employment.



CNCI Faces Challenges Scope of Education Efforts

However, CNCI stakeholders have not yet reached agreement on the scope of CNCI education efforts. According to the DHS official responsible for the CNCI education initiative, an interagency working group tasked with advising the education initiative has discussed the importance of broadening the scope of education efforts to include K-12, college, and graduate-level cybersecurity education. The DHS official responsible for cybersecurity education stated that one example of such efforts was the Centers of Academic Excellence in Information Assurance Education program; in this program, students can take better cybersecurity practices with them into the private sector, which is ultimately better for the federal government as a consumer of private sector goods and services. However, the White House has not yet approved the CNCI education implementation plan. According to the DHS official for cybersecurity education, some administration officials believe the plan should focus strictly on training the current workforce, rather than having a broader scope to include efforts for K-12 education and the college and graduate levels.

Experts have also discussed the challenge of expanding cybersecurity education and the federal cyber workforce. For example:

- The CSIS commission stated that there was neither a broad cadre of cyber experts nor an established cyber career field to build upon. It recommended increasing the supply of skilled workers, possibly through increasing scholarships, and developing a career path for cyber specialists in federal service.



CNCI Faces Challenges Scope of Education Efforts

- According to our expert panel, the federal government needs to publicize and raise awareness of the seriousness of the cybersecurity problem and to increase the number of professionals with adequate cybersecurity skills. Expert panel members stated that the cybersecurity discipline should be organized into concrete professional tracks through testing and licensing. Such tracks would increase the federal cybersecurity workforce by strengthening the hiring and retention of cybersecurity professionals.
- The White House policy review discussed education and workforce development as important parts of the national cybersecurity strategy. In particular, the policy review recommended
 - initiating a national public awareness and education campaign to promote cybersecurity;
 - expanding support for key education programs and research and development to ensure the nation's continued ability to compete in the information age economy; and
 - developing a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the federal government.



CNCI Faces Challenges Scope of Education Efforts

- The Partnership for Public Service, a non-profit policy group, recently released a study finding that the federal government faces major challenges in attracting, hiring, training, retaining, and effectively managing cybersecurity talent.¹⁵ They added that the federal government would be unable to combat cybersecurity threats without a more coordinated, sustained effort to increase cybersecurity expertise in the federal workforce.

Until agency officials agree on the scope of CNCI's education efforts, public awareness and broad cybersecurity education will not be fully addressed by the CNCI.

¹⁵Partnership for Public Service, *Cyber IN-Security: Strengthening the Federal Cybersecurity Workforce* (Washington D.C., July 2009).



Conclusions

The White House and federal agencies have taken a number of actions to establish and use interagency mechanisms in planning and coordinating CNCI activities, and these groups have used status meetings and other reporting mechanisms to track the implementation progress of CNCI's component projects. Beginning with the work of the National Cyber Study Group in brainstorming and gathering information from multiple federal sources, the management approach for the initiative has emphasized coordination across agencies.

While planning for CNCI has been broadly coordinated, the initiative faces challenges if it is to achieve its objectives related to securing federal information systems, which include reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats. Among other things, roles and responsibilities for participating agencies have not always been clearly defined, measures of effectiveness have not yet been established, and key issues—such as coordination with international entities and the governmentwide implementation of identity management and authentication—have not received strategic attention. These challenges have been highlighted by experts and in other recent reviews of federal cybersecurity strategies. Until they are addressed within CNCI, the initiative risks not fully meeting its objectives.



Recommendations for Executive Action

We are recommending that the Director of National Intelligence and the Director of the Office of Management and Budget address the challenges that CNCI faces in achieving its objectives related to securing federal information systems by taking the following six actions:

- better define roles and responsibilities of all key CNCI participants, such as the National Cyber Security Center, to ensure that essential governmentwide cybersecurity activities are fully coordinated;
- establish measures to determine the effectiveness of CNCI projects in making federal information systems more secure and track progress against those measures;
- establish an appropriate level of transparency about CNCI by clarifying the rationale for classifying information, ensuring that as much information is made public as is appropriate, and providing justification for withholding information from the public;
- establish a coordinated approach for the federal government in conducting international outreach to address cyber security issues strategically;
- establish a strategic approach to identity management and authentication, linked to HSPD-12 implementation, to provide greater assurance that only authorized individuals and other entities can gain access to federal information systems; and
- reach agreement on the scope of CNCI's education projects to ensure that an adequate cadre of skilled personnel is developed to protect federal information systems.



Agency Comments and Our Evaluation

We provided a draft of this briefing to OMB, ODNI, and the Department of State for review and comment. In comments provided via e-mail, an official in OMB's Office of E-Government and Information Technology agreed that federal cybersecurity policy has many areas that could use improvement but disagreed that these issues are all related to CNCI, noting that the CNCI was built upon existing cybersecurity activities within the federal government and did not eliminate or subsume other activities. We agree that CNCI was not intended to subsume all federal activities related to cybersecurity and have clarified our briefing to avoid a potential misunderstanding. Nevertheless, we believe that the challenges we identified remain of critical importance in determining whether CNCI can achieve its objectives related to securing federal information systems.

Regarding our briefing's discussion of the need to better define roles and responsibilities of federal entities in securing federal systems, OMB observed that specific roles and responsibilities for the various CNCI initiatives were clearly defined. We agree that, as described in our briefing, lead responsibility has been assigned for each of the CNCI initiatives. However, this observation does not diminish the larger challenge that CNCI faces in better establishing federal cybersecurity roles and responsibilities. For example, we note that, according to the then-acting director, the NCSC has not been fully operational and has had unclear responsibilities. OMB commented that NCSC's responsibilities would not overlap with other federal entities involved in incident detection and response; however, we disagree. US-CERT, for example, which handles incident response, engages in extensive cross-agency coordination, and it remains unclear how this function differs from the responsibilities planned for NCSC.



Agency Comments and Our Evaluation

Regarding international outreach, OMB noted that a formal “deconfliction” process exists among federal agencies regarding international issues. However, the challenge we identified is a larger issue, involving establishing a coordinated strategy among federal agencies, something that has not been undertaken as part of CNCI and that remains critical to its success.

Similarly, with regard to identity management and authentication, OMB stated the CNCI did not address this topic because it relied on the implementation of Homeland Security Presidential Directive 12 (HSPD-12). We disagree. The briefing acknowledges and discusses the role of HSPD-12 and notes that the CSIS commission and the White House Policy Review both agreed that further improvements were needed in this area.

OMB also provided technical comments that we have addressed as appropriate in the final briefing.



Agency Comments and Our Evaluation

The Director of Legislative Affairs of ODNI provided written comments on a draft of the briefing. In its comments, ODNI agreed that the challenges we identified should have been included or accounted for in CNCI but raised concern that the program should not be criticized for items that were not included in it. As previously stated, we agree that CNCI was not intended to subsume all federal activities related to cybersecurity and have clarified our briefing to avoid a potential misunderstanding. Nevertheless, we believe that the challenges we identified remain of critical importance in determining whether CNCI can achieve its objectives related to securing federal information systems. In addition, ODNI provided comments that were technical in nature, which we have addressed, as appropriate, in the final briefing.

The Director of the Office of Computer Security at the Department of State provided technical comments via e-mail that we have addressed as appropriate in the final briefing.

Appendix II: Comments from the Office of Management and Budget



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

Gregory Wilshusen
Director
The Government Accountability Office
441 G Street, Northwest
Washington, D.C. 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on your draft report, "CYBERSECURITY: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative" (GAO-10-338). We appreciate the work that the Government Accountability Office (GAO) has done in this area and we welcome GAO's interest in this area.

The Comprehensive National Cybersecurity Initiative (CNCI), created by National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), is a set of 12 discrete activities that were designed to coordinate with other existing Federal cybersecurity activities to protect the Federal Executive Branch agencies and departments from specific threats. The value of the CNCI was reinforced in the President's *Cyberspace Policy Review*.

As we explained in the technical comments that we provided to GAO staff on October 29, 2009, we do not concur with some of the findings, conclusions and recommendations in the report.

Findings and Conclusions:

With respect to the findings and conclusions made by GAO concerning better defining roles and responsibilities for agencies participating in the CNCI, we do not concur. The roles and responsibilities of agencies participating in the CNCI are clearly defined by NSPD-54/HSPD-23. For example, as illustrated in Table 1 in your report, lead agencies have been designated for each initiative. Lead agencies are held to implementation plans and report quarterly on their progress against goals.

In addition, the draft report cites the agencies' response to the July 2009 distributed denial of service attacks against some federal websites as an example of the confusion over roles and responsibilities for agencies participating in the CNCI. As we explained in the technical comments that we provided to GAO staff on October 29, 2009, the government's response to the incident was not an activity that fell under the roles and responsibilities under CNCI. Operational incident response management for civil executive branch departments and agencies is set forth in the Federal Information Security Management Act.

The draft report also states the view that there are “overlapping and uncoordinated” responsibilities regarding cyber information sharing and situational awareness. We do not agree. The National Computer Security Center is responsible for assisting with situational awareness across the government, public and private sectors. As the draft report notes, the other cyber security response centers are responsible for operational incident response.

The draft report also states the view that the role of the NCSC is unclear. We do not agree. As we explained in the technical comments we provided to GAO staff on October 29, 2009, NCSC coordinates incident information flowing between multiple operational incident response centers in the Federal Government. It does not handle incident detection and response, which is a responsibility of operational incident response centers. NCSC’s role was predicated on the implementation of the activities in initiative 5: Connecting the Centers. As these activities have been delayed, the implementation of the NCSC has also been delayed.

Finally, as we explained in the technical comments we provided to GAO staff on October 29, 2009, we also requested that you clarify the description of the interagency policy committee (IPC) to explain that IPCs are formal bodies that deal with interagency coordination in many areas. The IPC, in this case, operates under the National Security Council which is the advising and consenting party to NSPD-54/HSPD-23. IPCs are components of a decision structure established by Presidential Directive that includes both deputies and principals of agencies.

Recommendations:

Of the six recommendations that GAO makes in this report to the Director of the Office of Management and Budget, we do not concur with one and concur with five. We do not concur with the recommendation to better define roles and responsibilities of all key CNCI participants since, NSPD-54/HSPD-23 clearly defines roles and responsibilities for activities within the CNCI.

We concur with the recommendations related to the CNCI with the following comments:

1. *Recommendation: establish measures to determine the effectiveness of CNCI projects in making federal information systems more secure and track progress against those measures.*

Comment: As we explained in the technical comments we provided to GAO staff on October 29, 2009, establishment of performance measures has always been part of the planning for the CNCI once the initiatives were past the implementation stage.

2. *Recommendation: establish an appropriate level of transparency about CNCI by clarifying the rationale for classifying information, ensuring that as much information is made public as is appropriate, and providing justification for withholding information from the public.*

Comment: Consideration of the classification of information about the CNCI is already being done by the IPC responsible for CNCI oversight. We believe that is the correct venue for this activity.

Appendix II: Comments from the Office of Management and Budget

3. *Recommendation: reach agreement on the scope of CNCI's education projects to ensure that an adequate cadre of skilled personnel is developed to protect federal information systems.*

Comment: The IPC responsible for CNCI oversight has already completed a re-evaluation of the CNCI's education projects and has redefined their scope. We believe that the IPC is the correct and appropriate venue for this activity.

We concur with the two recommendations that are related to strategic challenges in areas that are not part of the CNCI with the following comments:

1. *Recommendation: establish a coordinated approach for the federal government in conducting international outreach to address cybersecurity issues strategically.*

Comment: This activity is already in existence within the appropriate IPC under the National Security Staff. We believe that this is the correct and appropriate venue for this activity.

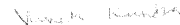
2. *Recommendation: continue development of a strategic approach to identity management and authentication, linked to NISPD-12 authentication, as initially described in the CIO Council's plan for implementing federal identity, credential, and access management so as to provide greater assurance that only authorized individuals and entities can gain access to federal systems.*

Comment: Such a strategic approach already exists in The Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, dated November 10, 2009. This document provides architecture and implementation guidance to agencies in implementing Federal identity management requirements.

The security of Federal information systems is a major concern of this Administration. Our nation's security and economic prosperity depend on the stability and integrity of our Federal communications and information infrastructure. Recognizing the challenges and opportunities, the President identified cybersecurity as one of the top priorities of his administration and directed a 60-day comprehensive review to assess U.S. policies and structures for cybersecurity. The President has also appointed Howard Schmidt as the Special Assistance to the President and Cybersecurity Coordinator to increase and sustain attention to cybersecurity.

Thank you again for the opportunity to comment on this draft report.

Sincerely,



Vivek Kundra
Federal Chief Information Officer

Appendix III: Comments from the Office of the Director of National Intelligence

Note: GAO comments regarding this letter appear at the end of this appendix.

See comment 1.

UNCLASSIFIED
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

JAN 22 2010

Mr. Gregory C. Wilshusen
Director, Information Security Issues
United States Government
Accountability Office
Washington, DC 20548

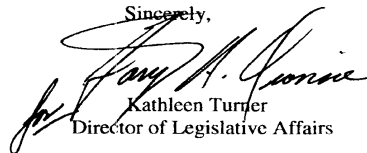
Dear Mr. Wilshusen:

(U) This responds to your request dated 30 Dec. 2009, for review of a draft GAO report, "CYBERSECURITY: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative", GAO 10-338, dated February 2010. This report relates to an inquiry originally initiated in February, 2009 on the Comprehensive National Cybersecurity Initiative (GAO Code 311019) by Ms. Janet A. St. Laurent, Managing Director, Defense Capabilities and Management United States Government Accountability Office.

(U) This office provided a detailed review of the body of this report on 4 November, 2009, under GAO Code 31101. Those recommendations remain largely unincorporated in this product. As a result, the concerns expressed in that communication remain and carry forward to this product as well. I request that your office refer back to those comments, incorporate them fully and adjust the report accordingly.

(U) If you have any questions regarding this matter, please do not hesitate to contact me at (703) 275-2473.

Sincerely,



Kathleen Turner
Director of Legislative Affairs

UNCLASSIFIED

GAO Comment

1. In its earlier comments, ODNI had raised concern that CNCI should not be criticized for items that were not included in it. As discussed in the letter, to avoid potential misunderstanding, we have clarified that two of the challenges we identified are not connected to specific CNCI projects but rather relate to additional cybersecurity activities that are necessary to achieve CNCI's overall goal of securing federal information systems.

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Davi M. D'Agostino at (202) 512-5431 or dagostinod@gao.gov.

Staff Acknowledgments

In addition to the individual named above, key contributions to this report were made by John de Ferrari (Assistant Director), Sherrie Bacon, Matthew Grote, Nick Marinos, Lee McCracken, David Plocher, Daniel Swartz, and Jeffrey Woodward.

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



USAF adds cyber training for recruits and officers

By DAN ELLIOTT (AP) – Apr 12, 2010

COLORADO SPRINGS, Colo. — The Air Force will train all new recruits in the basics of cyberwarfare and add more advanced schooling for others to help combat the growing threat of attacks on U.S. computer networks, a top commander said Monday.

Four-star Gen. Robert Kehler said details are still being worked out on a cyberwarfare component for basic training, but it would be brief, perhaps an hour or two total, and would cover only the fundamentals.

A more advanced, undergraduate-level training program will begin in June to train officers and enlisted personnel for a new Air Force career field in cyber operations, Kehler said.

He likened it to existing undergraduate training for pilots, navigators, missile operators and space operators.

Kehler, who heads the Air Force Space Command at Peterson Air Force Base in Colorado Springs, spoke to the annual National Space Symposium and in a separate interview. The Space Command oversees the Air Force's cyberwarfare operations.

Kehler said the basic training component would cover such basic precautions as using firewalls and passwords.

"We teach them at basic training fundamentals of an M-16 (rifle), for example, and an M-9 (pistol), and so we want them to know the fundamentals of the computer network that they're going to be operating in," he said.

The more advanced training will last six months and include skills currently taught to communications operators plus additional skills in computer networks and vulnerabilities. That will be followed by more specific training.

The first class will include about 16 officers. Kehler said several sessions are planned each year because the Air Force will need to produce about 400 officers annually with skills in cyberwarfare.

They will be assigned jobs across the Air Force, including the 24th Air Force, based in Lackland Air Force Base, Texas, a component of the Space Command responsible for cyberwarfare and Air Force computer networks.

Copyright © 2010 The Associated Press. All rights reserved.

Related articles

- [USAF adds cyber training for recruits and officers](#)
The Associated Press - Apr 12, 2010
- [Air Force To Begin Cyberwarfare Training](#)
RedOrbit - Apr 13, 2010
- [USAF adds cyber training for recruits, officers](#)
The Associated Press - Apr 12, 2010
- [More coverage \(1\) »](#)



[Add News to your Google Homepage](#)



Map



©2010 Google - [About Google News](#) - [Blog](#) - [Help Center](#) - [Help for Publishers](#) - [Terms of Use](#) - [Privacy Policy](#) - [Google Home](#)

Senate stalls cyber commander to probe digital war

By LOLITA C. BALDOR
The Associated Press
Monday, April 12, 2010; 6:16 PM

WASHINGTON -- When hackers a continent away attack a military computer system, using computers belonging to unsuspecting private citizens or businesses as cover, what are the rules when the U.S. fights back?

As U.S. officials struggle to put together plans to defend government networks, they are faced with questions about the rippling effects of retaliation. Taking action against a hacker could affect foreign countries, private citizens or businesses - ranging from hospitals to power plants - whose computers might get caught up in the electronic battle.

Difficult questions about how and when the U.S. military conducts electronic warfare have stalled the creation of the Pentagon's Cyber Command for months as senators dig into such scenarios involving the rules of the digital battlefield, according to congressional officials.

Government leaders have grown increasingly alarmed as U.S. computer networks face constant attacks, including complex criminal schemes and suspected cyber espionage by other nations, such as China. But the nation's ability to protect

its networks and respond to attacks are largely kept secret because of national security concerns and the government's slowly evolving cyber security plans.

Electronic warfare by U.S. forces is not new. For example, in the Iraq war, U.S. forces jammed cellular phone networks in Fallujah in 2004 to disrupt communications between enemy insurgents, and interrupted radio signals designed to trigger roadside bombs.

But U.S. officials refuse to discuss any current offensive cyber operations or monitoring, particularly anything that involves other countries or terror organization.

The nomination of Lt. Gen. Keith Alexander to head Cyber Command has given senators leverage to delve into the

Advertisement



HEARTLAND QUALITY
OMAHA STEAKS
SINCE 1917

SAVE
up to **64%**

Plus, get
3 FREE Gifts Special Code: **45069ZWN**

To order: www.OmahaSteaks.com/print71
or call 1-877-586-4455

http://www.washingtonpost.com/wp-dyn/content/article/2010/04/12/AR2010041203539_pf.html

Print Powered By  FormatDynamics

Senate stalls cyber commander to probe digital war

complex world of cyber warfare. Later this week, a Senate committee will face off with Alexander during a hearing on his nomination.

The Cyber Command would oversee military networks and take on what U.S. authorities see as a growing national security threat - cyber terrorists looking to steal sensitive technologies, disrupt critical services, or infiltrate classified networks.

In recent months, according to several congressional officials, senators have called in defense officials for meetings, gathered for a Cyber 101 session with a top general, and put together dozens of pages of questions for the Pentagon and Alexander, digging into the military's rule book on electronic warfare.

In response, the Pentagon drafted carefully worded responses, walking a delicate line between satisfying the Senate's concerns while closely guarding the high-tech secrets of its digital weaponry, said the officials, who spoke on condition of anonymity to discuss internal deliberations.

One concern involves Alexander's position as head of the National Security Agency, which oversees electronic intelligence-gathering. Lawmakers and others question whether the secretive spy agency should have control over cyber

issues.

"We are obviously concerned about the nomination of Lt. Gen. Alexander," said Marc Rotenberg, executive director of the Washington-based Electronic Privacy Information Center. "The NSA has broad authority to conduct electronic surveillance against U.S. citizens and the oversight system simply does not work."

Another issue, Rotenberg said, is that the NSA is seeking to expand its ability to monitor domestic communications through the development of Einstein 3, a government network monitoring system currently being tested. The program would both detect and take action against cyber attacks on federal systems.

Homeland Security Department officials began the Einstein 3 trial program late last summer, and started testing it on one federal agency's network traffic a

Advertisement



Send flowers
for any occasion

Bouquets \$19.99
from \$19.99^{+s/h}

ProFlowers[®]
Order ONLY at
proflowers.com/happy
or call 1-877-888-0688

http://www.washingtonpost.com/wp-dyn/content/article/2010/04/12/AR2010041203539_pf.html

Print Powered By  FormatDynamics

Senate stalls cyber commander to probe digital war

couple weeks ago. Officials have not identified which agency is being used for the test, but have stressed all along that extensive privacy protections are in place.

James Lewis, a cybersecurity expert and senior fellow at the Washington-based Center for Strategic and International Studies, downplayed the privacy concerns. The main issues, he said, involve who can authorize an offensive cyber strike, what are the command's legal authorities, and how will it interact with the NSA and DHS when other government or critical networks are attacked.

Lewis said Cyber Command, which will report to U.S. Strategic Command based in Omaha, Neb., would likely support the other agencies, much like the North American Aerospace Defense Command supports the Federal Aviation Administration. NORAD often launches fighters during aviation incidents - such as the bomb scare triggered by a Qatari diplomat earlier this week when the man reportedly slipped into the bathroom for a smoke and joked about trying to set his shoes on fire.

Several congressional officials said there is no strong opposition to Alexander taking on the dual NSA and Cyber Command posts. Still, senators have many questions.

On the Net:

Defense Department:<http://www.defenselink.mil>

Advertisement

Own a new computer for just \$29.99* per week!

Call today to get the computer of your dreams, and improve your credit at the same time.



If you can afford a weekly payment of just \$29.99* for just 12 months, then you're already approved for a brand new Desktop or HP™ Computer, guaranteed!

1-877-294-3988

GIVE US A CALL TODAY!

*Prices start at \$29.99 but may vary by model.

http://www.washingtonpost.com/wp-dyn/content/article/2010/04/12/AR2010041203539_pf.html



1 of 5 DOCUMENTS

Copyright 2006 Factiva®, from Dow Jones
All Rights Reserved

Dow Jones Factiva

(Copyright (c) 2006, Dow Jones & Company, Inc.)

THE WALL STREET JOURNAL

The Wall Street Journal

December 22, 2006 Friday

SECTION: Pg. A6

LENGTH: 762 words

HEADLINE: Politics & Economics: Smartmatic to Shed U.S. Unit, End Probe Into Venezuelan Links

BYLINE: By Bob Davis

BODY:

WASHINGTON -- Voting-machine company Smartmatic Corp. said it would sell its U.S. subsidiary to end a review by the Committee on Foreign Investment in the U.S. into whether Smartmatic is partially owned by the Venezuelan government.

Smartmatic, owned by Venezuelan entrepreneurs who split their time between Caracas and Boca Raton, Fla., portrayed itself as the latest victim of a U.S. protectionist response to foreign investment in sensitive industries. Earlier this year, a company owned by the government of Dubai, a Gulf emirate that is part of the United Arab Emirates, drew opposition in Congress and some media outlets with plans to buy a company that runs commercial operations at several U.S. ports. The company later sold the port-operations business.

"Given the current climate of the United States marketplace, with so much public debate over foreign ownership of firms in an area that is viewed as critical U.S. infrastructure -- election technology -- we feel it is in both companies' best interests to move forward as separate entities with separate ownership," Smartmatic said. The company said it plans to sell Sequoia Voting Systems Inc., headquartered in Oakland, Calif., which it purchased in early 2005 for \$16 million.

The Committee on Foreign Investment, known as the CFIUS, reviews foreign acquisitions to see if they pose national-security concerns. Normally, such reviews are conducted before deals close. The Smartmatic acquisition drew attention earlier this year because of concerns that the government run by Venezuelan President Hugo Chavez, an opponent of U.S. policy, owns a stake in the company.

Since its purchase by Smartmatic, Sequoia's sales have risen sharply to a projected \$200 million in 2006, said Smartmatic's chief executive, Anthony Mugica. He said the firm has a "healthy" profit but didn't provide a specific figure. Nevertheless, the CFIUS investigation, as well as a separate Justice De-

partment probe into whether Smartmatic had paid bribes in Venezuela, had become a "distraction" for senior management, Mr. Mugica said.

With the 2008 election on the horizon, Mr. Mugica said, "it would be an extremely big mistake to not capitalize on the opportunity [of selling voting-machine equipment] by having a handicap, even if it was only a fantasy or a myth about Sequoia."

Sequoia voting machines were used in 16 states and the District of Columbia in 2006. Smartmatic, which has revenue of about \$100 million, focuses on Venezuela and other markets outside the U.S. After selling Sequoia, Mr. Mugica said, he hoped Smartmatic would work with Sequoia on projects in the U.S., though Smartmatic wouldn't take an equity stake.

The proposed sale may dim the spotlight on the Justice Department probe and make it easier to resolve. Among the issues the department is looking at are whether Smartmatic paid bribes to Venezuelan officials to win an election contract in 2004 and failed to pay taxes owed in the U.S. Smartmatic said it is cooperating with that probe and that the Justice Department hasn't issued any subpoenas to Smartmatic employees.

Jeffrey Bialos, a lawyer for Smartmatic, said the Justice Department investigation didn't play into its sales decision. Rather, he said, the attitude in the U.S. to foreign acquisitions had hardened since the Sept. 11, 2001, terror attacks.

A spokeswoman for the Treasury, which takes the lead on matters regarding the CFIUS, said the committee agreed to end the Smartmatic review but added that "CFIUS will closely monitor the sale process."

Smartmatic came to prominence in 2004 when its machines were used in an election to recall President Chavez, which Mr. Chavez won handily -- and which the Venezuelan opposition said was riddled with fraud. Smartmatic put together a consortium to conduct the recall elections, including a company called Bizta Corp., in which Smartmatic owners had a large stake. For a time, the Venezuelan government had a 28% stake in Bizta in exchange for a loan.

Bizta paid off the loan in 2004, and Smartmatic bought the company the following year. But accusations of Chavez government control of Smartmatic never ended, especially since Smartmatic scrapped a simple corporate structure, in which it was based in the U.S. with a Venezuelan subsidiary, for a far more complex arrangement. The company said it made the change for tax reasons, but critics, including Rep. Carolyn Maloney (D., N.Y.) and TV journalist Lou Dobbs, pounded the company for alleged links to the Chavez regime.

License this article from Dow Jones Reprint Service

NOTES:

PUBLISHER: Dow Jones & Company, Inc.

LOAD-DATE: December 22, 2006



FOR IMMEDIATE RELEASE

CONTACTS:

Michelle M. Shafer
Sequoia Voting Systems
Vice President, Communications & External Affairs
800.347.4702
mshafer@sequoiavote.com

Mitch Stoller
Group SJR
212.751.3341
mstoller@groupsjr.com

**U.S. VOTING TECHNOLOGY LEADER SEQUOIA VOTING SYSTEMS
ANNOUNCES NEW CORPORATE OWNERSHIP**

Sale Creates 100% American-Owned and Independent Company

DENVER, COLO. (November 8, 2007) – Leading voting technology provider Sequoia Voting Systems is pleased to announce the sale of the company to a group of private U.S. investors led by Sequoia's current executive management team.

"Sequoia is an innovative company with a century-long history; hard-working and talented employees; proven products; a solid balance sheet; essentially no debt, a corporate structure that provides flexibility; an extensive customer base and a very bright future," said Jack Blaine, Sequoia President & CEO. "I am very excited and hopeful about the tremendous possibilities and numerous opportunities that lay ahead for Sequoia given the company's new structure and the completion of this sale process."

The investment group, led by Sequoia President & CEO Jack Blaine and company Chief Financial Officer Peter McManemy, purchased Sequoia from former parent company Smartmatic Corporation for an undisclosed sum. As with most transactions involving two private entities, the specific terms of the sale are not being disclosed. However, this transaction does include investment by the management team, a small loan and an earn-out. This scenario provides an excellent financial structure for Sequoia to leverage and completely eliminates Smartmatic's ownership, control and operational rights of any kind in Sequoia.

On December 22, 2006, Smartmatic Corporation announced the company's intention to sell Sequoia Voting Systems. At that time, Smartmatic CEO Antonio Mugica stated, "Sequoia's customer base has grown substantially and its revenues have increased four-fold. However, given the current climate of the United States marketplace with so much public debate over foreign ownership of firms in an area that is viewed as critical U.S. infrastructure – election technology – we feel it is in both companies' best interests to move forward as separate entities with separate ownership. As part of this process, we plan to sell our Sequoia Voting Systems ownership."

Sequoia Voting Systems worked for many months with Smartmatic to find an appropriate situation that would be a win-win for both companies.

Given Sequoia's strong position in the US electoral market and significant opportunities therein, many buyers expressed interest in Sequoia. Smartmatic selected this team to purchase Sequoia as they believe in the ability of Sequoia's current management team to perform as successfully as they have in the past, which will allow Smartmatic to capitalize on the earn-out purchase plan.

Led by Jack Blaine and Peter McManemy, the Sequoia management team has both the deep experience in the highly complex, ever-changing and regulated voting industry and the expertise in mission critical software and change management necessary to ensure future success.

"This is a great opportunity for Sequoia's customers, suppliers and employees," said Blaine. "This management team knows the elections industry inside and out and is not deterred by the challenges and changes inherent to this dynamic industry. In fact, we are motivated and excited by these challenges and changes."

Sequoia currently supplies voting technology and services to jurisdictions throughout 17 states and the District of Columbia.

Sequoia's ownership changes will have no material impact on Sequoia's current customers, employees, suppliers or the company's business operations.

About Sequoia Voting Systems (www.sequoiavote.com)

Sequoia Voting Systems is an American-owned election technology company with major offices in Denver, Colorado; Jamestown, NY and Oakland, California with over a 100-year history of providing accurate, reliable and innovative voting solutions dating back to the nation's first lever-based mechanical voting equipment in the 1890s. Sequoia provides comprehensive election technology products, customized training options, ballot layout and printing services and complete implementation and support programs to its state and local government customers throughout the United States. Sequoia's product suite includes a comprehensive election management system, precinct-based optical scan voting units, high-speed central count optical scan ballot readers, and full-face and paginating touch screen electronic voting equipment with optional printers that produce voter verified paper records. Sequoia's voting equipment is currently used by hundreds of jurisdictions throughout 17 states and the District of Columbia.

#

5/28/04 Miami Herald 1A
2004 WLNR 19455271

Miami Herald (FL)
Copyright 2004 The Miami Herald

May 28, 2004

Section: Front

VENEZUELA OWNS STAKE IN BALLOTS

RICHARD BRAND AND ALFONSO CHARDY, rbrand@herald.com

CARACAS A large and powerful investor in the software company that will design electronic ballots and record votes for Venezuela's new and much criticized election system is the Venezuelan government itself, The Herald has learned.

Venezuela's investment in Bizta Corp., the ballot software firm, gives the government 28 percent ownership of the company it will use to help deliver voting results in future elections, including the possible recall referendum against President Hugo Chávez, according to records obtained by The Herald.

The deal to scrap the country's 6-year-old machines - for a \$91 million system to be built by two fledgling companies that have never been used in an election before - was already controversial among Chávez opponents who claimed it was a maneuver to manipulate votes amid growing political turmoil.

Chávez opponents told The Herald on Thursday they were stunned to learn the government has a proprietary stake in a company critical to the election process.

"The Venezuelan state? Are you kidding?," said Jesús Torrealba, an official in the Democratic Coordinator opposition group. "It impugns the credibility of the process. That is shocking."

Government officials insist the investment is an effort to help support private enterprise and its interest in a ballot software company is merely coincidental, one of a dozen such investments made to help struggling companies.

"The whole process led to a decision that was best for Venezuela," said Bernardo Alvarez, Venezuela's ambassador in Washington.

But Venezuela is a nation bitterly polarized by Chávez's leftist populist rule. Nearly every move by the government is scrutinized by opponents who accuse Chávez of trying to impose an authoritarian regime.

GOVERNMENT FUNDS

Until a year ago, the Bizta Corp. was a struggling Venezuelan software company with barely a sales deal to its

name, records show. Then, the Venezuelan government - through a venture capital fund - invested about \$200,000 and bought 28 percent of it.

The government's investment in Bizta made Venezuela Bizta's largest single shareholder and, ultimately, its most important client.

The decision to replace the \$120 million system built by Omaha-based Election Systems & Software was made Feb. 16 under unusual circumstances. Two of the five National Electoral Council members sympathetic to the opposition complained that they had been largely shut out of the process.

"The selection process was secret and it didn't allow us to get any information about the bidders and their products," board member Sobella Mejías said after the decision.

Other members knew about the government's investment, according to one member who asked not to be identified.

The new system is to be built by the Smartmatic Corp., which is incorporated in Florida, and programmed by Bizta, which also is registered in Florida and Venezuela.

Pro-Chávez government officials and company executives interviewed by The Herald say the Smartmatic-Bizta machines are among the most secure in the world, and that the government's investment in Bizta was unrelated to Bizta's bid for the voting machine contract.

"The companies that were chosen have the highest technical capacity," said Alvarez, the ambassador. "In Venezuela there have been many fair elections and there will be many more fair elections."

But the Atlanta-based Carter Center, which has observed every major Venezuelan electoral process since Chávez's election in 1998, said the disclosure of the government's role in Bizta reinforces the need for independent election audits.

"What we look at in any electoral process is whether each of the components is transparent and auditable. In this case, we would include these new machines," said Jennifer McCoy, who is leading the Carter Center's mission in Venezuela. She said she was unaware of the government's investment in Bizta.

Even without the political implications, the use of electronic voting machines has been widely debated since the United States' 2000 presidential election. Stanford University Professor David Dill, who has studied voting machines but is not specifically knowledgeable about the new Venezuelan system, said almost any programmed electronic machine is subject to possible manipulation.

"People just don't understand how easily these machines could fail to record votes accurately - even by being 'fixed,'" he said.

PAPER TRAIL

Smartmatic does produce a paper trail of votes as well, but Venezuelan government critics claim it will be useless since an election recount would be supervised by the Electoral Council, perceived as pro-Chávez.

The National Electoral Council members have hailed Bizta's software-writing role as contributing to Venezuelan "sovereignty" over their voting system, which replaces American-designed machines. Chávez, an outspoken critic of U.S. policy, is viewed as leftist and anti-American.

According to Bizta's 2002 financial statement, the most recent one filed by the company in Venezuela, it was then a dormant firm that had no sales and was slowly losing money.

In June 2003, however, a venture capital company called Sociedad de Capital de Riesgo (SCR) invested about \$200,000 in Bizta. The SCR is owned by the Venezuelan government's Industrial Credit Fund.

In January, a top official in Venezuela's science ministry, Omar Montilla, joined Bizta's board of directors to represent the government's three million shares, records show.

Montilla, who is one of five directors, canceled a meeting with The Herald and did not reply to repeated Herald queries.

One month after Montilla joined the board, the National Electoral Council awarded Bizta and partners Smartmatic and CANTV the \$91 million contract to develop new voting machines. Bizta was hired to write the electronic code that configured the names and parties of candidates on the touch screens. Smartmatic would build and design the machines. CANTV, the publicly held phone company, would provide the phone lines for the system and election-day technical support.

The venture is largely the work of two little-known Venezuelan engineers: Antonio Mugica Rivero and Alfredo Anzola Jaumotte, childhood friends and recent engineering school graduates.

Mugica, 30, is the president of Smartmatic and a founder of Bizta. Anzola, 30, is the president of Bizta and the vice president of Smartmatic, corporate records from Venezuela show.

NO CONNECTIONS

Both executives say they have no political allegiances. Neither signed a petition drive seeking Chávez's recall.

Anzola initially told The Herald that one of the reasons the electoral council selected the group was that it had no connection to either the government or the opposition.

When told in a subsequent interview in Caracas that Bizta papers showed the government had an investment in his company through SCR, Anzola and Mugica said they viewed the investment as a loan.

"We really don't want to be involved in politics," said Wladimir Serrano, head of the government's venture capital fund. "Our role is strictly financial and technical."

Bizta "remains a private company, with some government shares but without any say on our part on its day to day activities or its strategic programs and policies," Serrano said.

SUBSTANTIAL POWER

But Harvard Professor Ricardo Hausmann, a former Venezuelan official who also has worked as the chief economist of the Inter-American Development Bank, said any investor holding a 28 percent stake in a company would likely have substantial power to make decisions.

"For example, Verizon is the largest shareholder in CANTV, holding 28 percent, and it has control of the company's management," said Hausmann, who sits on the CANTV board. With Bizta, "The government's influence will

depend on the arrangement between the government and other shareholders."

SCR's stock purchase in Bizta was part of a broader effort to help start-up companies that could bring Venezuela international prestige in a wide range of industries, Serrano said.

He provided a list of a dozen other companies in which SCR has invested.

Most of the 20,000 Smartmatic-Bizta machines will be delivered over the summer from the factory in Italy, officials say.

Company Facts

Three companies will build and execute Venezuela's new touch-screen voting system. Two are incorporated in Florida, though neither does most of its business here.

* Smartmatic Corp., which will build the machines, incorporated in Florida in 2000 and lists its world headquarters at 6400 Congress Ave. in Boca Raton. Its president is Antonio Mugica Rivero, 30, and its vice president is Alfredo Anzola, 30.

* Bizta Corp., which will provide software for the new machines, incorporated in Florida in 2001, and lists its address as 19591 Dinner Key Dr., Boca Raton, a residential property owned by Mugica's father. Mugica is listed as president, and Anzola is vice president, according to Florida records. Venezuelan records, however, indicate Anzola is president. In Caracas, Bizta shares its office with Smartmatic.

* CANTV, Venezuela's publicly held phone company, will provide phone lines to connect the system and election day technical support. It would have been part of any voting system selected for the elections contract.

---- INDEX REFERENCES ----

COMPANY: INTER AMERICAN DEVELOPMENT BANK; SMARTMATIC CORP; SMARTMATIC; HARVARD

NEWS SUBJECT: (Funding Instruments (1FU41); Venture Capital (1VE73); Corporate Funding (1XO17))

INDUSTRY: (Financial Services (1FI37))

REGION: (USA (1US73); Americas (1AM92); Venezuela (1VE06); Florida (1FL79); North America (1NO39); South America (1SO03); Latin America (1LA15))

Language: EN

OTHER INDEXING: (BALLOTS; BIZTA; BIZTA CORP; CANTV; CARTER CENTER; CONGRESS AVE; CONNECTIONS; DEMOCRATIC COORDINATOR; DINNER KEY; ELECTION SYSTEMS SOFTWARE; ELECTORAL COUNCIL; HARVARD; HERALD; INDUSTRIAL CREDIT FUND; INTER AMERICAN DEVELOPMENT BANK; NATIONAL ELECTORAL COUNCIL; SCR; SMARTMATIC; SMARTMATIC BIZTA; SMARTMATIC CORP; DE CAPITAL DE RIESGO (SCR); STAKE; STANFORD UNIVERSITY) (Alfredo Anzola; Alfredo Anzola Jaumotte; Alvarez; Antonio Mugica Rivero; Anzola; Bernardo Alvarez; Boca Raton; Chávez; David Dill; Hausmann; Hugo Chávez; Jennifer McCoy; Jesús Torrealba; Montilla; Mugica; Mugica Rivero; Omar Montilla; Ricardo Hausmann; Serrano; Sobella Mejías; Wladimir Serrano)

EDITION: Final

Word Count: 1850
5/28/04 MIAMIHD 1A
END OF DOCUMENT

THE TECHNICAL GUIDELINES DEVELOPMENT COMMITTEE

- The Technical Guidelines Development Committee was established under the Help America Vote Act of 2002 (Pub. L. No. 107-252) and is governed by the Federal Advisory Committee Act (FACA), which sets forth procedural requirements for establishment and operation of advisory committees.

The Role of the Committee

- Under the FACA, the Committee may be advisory only. The Committee has no “operational” functions“ such as making or implementing Government decisions. When in doubt about the propriety of a particular Committee activity, members should ask the Committee’s Designated Federal Officer (DFO).
- The Committee’s advisory duties are determined by statute which provides that the general purpose of the Committee is to assist the Executive Director of the Election Assistance Commission in the development of voluntary voting system guidelines.
- The Committee shall provide its first set of recommendations to the Executive Director not later than 9 months after all of its members have been appointed.
- The Committee shall cause to have published in the Federal Register any guidelines on voluntary voting systems that are adopted by the Commission.

The Role of the Members

- All members are appointed by and serve at the pleasure of the Commission and the Director of the National Institute of Standards and Technology.
- The Committee may not advise Congress directly, or engage in grassroots lobbying activities because these activities are outside the scope of the charter, and may implicate other prohibitions against grassroots lobbying that apply to Federal agencies and employees in general. Of course, this does not affect any Committee member’s activities in other capacities, such as a private citizen.
- This Committee includes two types of members: those who serve in an individual capacity as subject matters experts, and those who serve in a representative capacity on behalf of a particular organization. The determination of the capacity in which a member serves is made by the Commission, which will inform each member as to his or her particular capacity.

- Members who serve in an individual, expert capacity are Special Government Employees (SGEs) under 18 U.S.C. § 208, and are subject to Federal conflict of interest statutes and rules. As such, they are prohibited from participating in particular matters that may have a direct and predictable effect on their financial interests or on those of a spouse, minor child, or general partner.
- SGEs also may not be Registered Agents under the Foreign Agents Registration Act (22 U.S.C. § 611 et seq.). The responsibility for determining whether any particular member is required to register as a foreign agent under this statute lies with the individual and not the Commission.
- Members who serve in a representative capacity are not subject to the conflict of interest statutes, but must still adhere to rules designed to prevent using a public position for private gain, including abuse of Government affiliation, resources, and information.
- Advice on standards of conduct matters for both SGEs and representatives will be provided by the Election Assistance Commission

Meetings of the Committee

- The Committee shall not act in the absence of a quorum which is defined as a simple majority of the members of the Committee not having a conflict of interest in the matter being considered by the Committee, except that, if the number of members on the Committee is even, half will suffice.
- All Committee meetings must be called by a Federal officer or employee (usually the DFO), announced to the public in advance, and be open to the public. While limited exceptions to the open meeting requirement exist, they must be based on applicable law. Closed meetings must be approved in advance by the Election Assistance Commission.
- Meetings should allow a reasonable opportunity for public comments. The public may also file written statements with the Committee at any time.
- All materials made available to the Committee, prepared for the Committee, or prepared by members of the Committee, as well as minutes and transcripts of meetings, will be available to the public in a reading room format (except that those materials that would qualify for withholding under the exemptions to the Freedom of Information Act shall be removed before materials are made available to the public).
- Meetings may be held in person, via videoconference or conference call, so long as the public is afforded contemporaneous access to the deliberations.

- A meeting does not occur when Committee members communicate on purely logistical or administrative matters, such as holding a conference call with the DFO to schedule a meeting.

Subcommittees

- Consistent with the FACA, the Election Assistance Commission will create any subcommittees that may be necessary to accomplish the Committee's function.
- Subcommittees which do not function independently of the Committee are not required to be separately chartered, but are subject to prior written approval of the Commission before convening.
- Independent subcommittees, or subcommittees that contemplate using non-members, will have to be looked at individually to determine whether they need to be separately chartered to comply with the FACA.
- Subcommittee reports, findings, and recommendations developed during subcommittee meetings must be forwarded to the full Committee, which must actually deliberate on these materials at a meeting that complies with the FACA prior to advising the Government based on the subcommittee's work.

Administrative Matters

- Administrative support for the Committee is provided by the Election Assistance Commission.
- Under the Help America Vote Act, the National Institute of Standards and Technology will provide technical assistance to the Commission.
- Members are not compensated for their services, but travel (including per diem in lieu of subsistence) may be paid for upon request. All Government-funded travel must be at the Government's request and must involve the provision of a direct service to the Government, such as convening to advise Government officials on Government matters. Reimbursement is set at the rates that apply to Federal employees under the Federal Travel Regulations.
- Election Assistance Commission attorneys provide legal advice to the Commission, including the DFO. With the exception of standards of conduct issues, they cannot serve as legal advisors to Committee members.

- Questions should be directed to the Committee's DFO. If the DFO cannot answer them, that person will consult with Commission attorneys and respond to the Committee member.

**CHARTER OF THE
U.S. ELECTION ASSISTANCE COMMISSION
TECHNICAL GUIDELINES
DEVELOPMENT COMMITTEE**

ESTABLISHMENT:

In accordance with the requirements of Section 221 of the Help America Vote Act of 2002 (P. L. 107-252), hereinafter referred to as the Act, the Election Assistance Commission (the "Commission") hereby Charters the Technical Guidelines Development Committee (the "Committee"), pursuant to the Federal Advisory Committee Act, 5 U.S.C. App. 2.

OBJECTIVES AND DUTIES:

Pursuant to 42 U.S.C. § 15361(b)(1), the Committee will act in the public interest to assist the Executive Director of the Commission in the development of the voluntary voting system guidelines.

MEMBERS AND CHAIRPERSON:

Membership: shall be composed of:

1. The Director of the National Institute of Standards and Technology (NIST) who shall serve as its chair.
2. A group of 14 other individuals appointed jointly by the Commission and the Director of NIST, consisting of the following:
 - A. An equal number of each of the following:
 - i. Members of the Standards Board,
 - ii. Members of the Board of Advisors,
 - iii. Members of the Architectural and Transportation Barrier, and Compliance Board (Access Board).
 - B. A representative of the American National Standards Institute.
 - C. A representative of the Institute of Electrical and Electronics Engineers (IEEE).
 - D. Two representatives of the (National Association of State Election Directors (NASSED) selected by such Association who are not members of the Standards Board or Board of Advisors, and who are not of the same political party.
 - E. Other individuals with technical and scientific expertise relating to voting systems and voting equipment.

Terms of service; vacancies:

1. Members of the Committee shall serve for a term of two (2) years, and may serve for a longer period only if reappointed for an additional term or terms. A term shall commence on the date this Charter was filed (see below).
2. A member of the Committee who has not been reappointed at the end of his or her term shall continue to serve on the Committee until such time as he or she is either reappointed or replaced.
3. Any vacancy in the Committee shall be filled in the manner in which the original appointment was made.
4. If an individual is appointed to fill a vacancy, that individual shall serve on the Committee for the remainder of the term for which the vacancy existed.

ADMINISTRATIVE PROVISIONS:

1. The Committee shall report to the Executive Director of the Commission.
2. Selected staff within NIST's Information Technology Laboratory will provide staff support for the Committee.
3. The Committee shall meet as necessary to carry out the work, duties and responsibilities of the Committee. Chair of the EAC or the Chair of the TGDC may call a meeting of the Committee.
4. Members of the Committee shall not be compensated for their services, but will, upon request, be allowed travel and per diem expenses in accordance with 5 U.S.C. 5701 et seq., while attending meetings of the Committee or subcommittees thereof, or while otherwise performing duties at the request of the Chair, while away from their homes or regular places of business.
5. The Committee shall function solely as an advisory body, in accordance with the provisions of the Federal Advisory Committee Act.
6. The annual cost of operating the Committee is estimated at \$159,000.00, including all direct and indirect expenses. It is estimated that one FTE will be required to support the TGDC.
7. The Committee shall not act in the absence of a quorum, which shall consist of a simple majority of the members of the Committee not having a conflict of interest in the matter being considered by the Committee, except that, if the number of members on the Committee is even, half will suffice.
8. The EAC will create any subcommittees of the TGDC that may be necessary to accomplish the TGDC's function. In addition, the EAC will establish such operating procedures as required

to support the TGDC, consistent with the Federal Advisory Committee Act, as amended.

DURATION:

While the duration of the Committee is continuing, the Charter shall be renewed every two years from the date of filing.

CHARTER FILING DATE:

This Charter was filed on the 12 day of August, 2008.

Signed:



Donetta Davidson, Commissioner,

U.S. Election Assistance Commission

For Direct Consolidation Loans First Disbursed On or After October 1, 1998 and For Which the Application Was Received Before October 1, 1998

The interest rate for Direct Subsidized and Unsubsidized Consolidation Loans is the bond equivalent rate of the 91-day Treasury bills auctioned at the final auction held before June 1 plus 2.3 percent. However, during in-school, grace, and deferment periods, the interest rate formula is the bond equivalent rate of the 91-day Treasury bills auctioned at the final auction held before June 1 plus 1.7 percent. These interest rates may not exceed 8.25 percent during any period. From July 1, 2007, to June 30, 2008, the interest rate for Direct Subsidized and Unsubsidized Consolidation Loans that were first disbursed on or after October 1, 1998 and for which the application was received before October 1, 1998, is 6.62 percent (4.92 percent plus 1.7 percent) during in-school, grace, and deferment periods and 7.22 percent (4.92 percent plus 2.3 percent) during all other periods.

The interest rate for Direct PLUS Consolidation Loans is the bond equivalent rate of the 91-day Treasury bills auctioned at the final auction held before June 1 plus 3.1 percent. These interest rates may not exceed 9.0 percent during any period. From July 1, 2007, to June 30, 2008, the interest rate for Direct PLUS Loans and Direct PLUS Consolidation Loans that were first disbursed on or after October 1, 1998 and for which the application was received before October 1, 1998, is 8.02 percent (4.92 percent plus 3.1 percent) during all periods.

For Direct Consolidation Loans For Which the Application Was Received On or After October 1, 1998, and Before February 1, 1999

The interest rate for Direct Consolidation Loans for which the application was received on or after October 1, 1998 and before February 1, 1999 is the bond equivalent rate of the 91-day Treasury bills auctioned at the final auction held before June 1 plus 2.3 percent. These interest rates may not exceed 8.25 percent during any period. From July 1, 2007, to June 30, 2008, the interest rate for Direct Consolidation Loans for which the application was received on or after October 1, 1998 and before February 1, 1999, is 7.22 percent (4.92 percent plus 2.3 percent) during all periods.

For Direct Consolidation Loans For Which the Application Was Received On or After February 1, 1999

The interest rate for Direct Consolidation Loans for which the application was received on or after February 1, 1999, is the lesser of 8.25 percent, or the weighted average of the loans consolidated, rounded to the nearest higher $\frac{1}{8}$ of one percent.

Electronic Access to This Document: You may view this document, as well as all other documents of this Department published in the **Federal Register**, in text or Adobe Portable Document Format (PDF) on the Internet at the following site: <http://www.ed.gov/news/federegister>.

To use PDF you must have Adobe Acrobat Reader, which is available free at this site. If you have questions about using PDF, call the U.S. Government Printing Office (GPO), toll free at 1-888-293-6498; or in the Washington, DC area at (202) 512-1530.

Note: The official version of this document is the document published in the **Federal Register**. Free Internet access to the official edition of the **Federal Register** and the Code of Federal Regulations is available on GPO Access at: <http://www.gpoaccess.gov/nara/index.html>.

Program Authority: 20 U.S.C. 1087 *et seq.*

Dated: October 31, 2007.

Lawrence A. Warder,

Acting Chief Operating Officer, Federal Student Aid.

[FR Doc. E7-21807 Filed 11-5-07; 8:45 am]

BILLING CODE 4000-01-P

ELECTION ASSISTANCE COMMISSION

Proposed Guidance on Voluntary Voting System Guidelines

AGENCY: United States Election Assistance Commission.

ACTION: Notice of TGDC draft recommendations of Voluntary Voting System Guidelines and request for comments.

SUMMARY: The Help America Vote Act of 2002 (HAVA) (Pub. L. 107-252, October 29, 2002) established the U.S. Election Assistance Commission (EAC). Section 202 of HAVA directs the EAC to adopt voluntary voting system guidelines (VVSG) and to provide for the testing, certification, decertification, and recertification of voting system hardware and software. The VVSG provides specifications and standards against which voting systems can be tested to determine if they provide basic functionality, accessibility, and security capabilities. Section 221 of HAVA

mandates the creation of the Technical Guidelines Development Committee (TGDC) to assist the EAC in developing its voluntary voting system guidance. The TGDC has recommended standards to the EAC. These recommended standards were submitted by the TGDC to the EAC's Executive Director pursuant to section 221 of HAVA.

As part of its development process the EAC is seeking public comment on the TGDC's recommended standards. The EAC encourages the public to offer specific and detailed comments on all aspects and sections of the requirements. The EAC is particularly interested in receiving comments on three distinct issues:

- (1) The concept of Software Independence and the corresponding requirements for Independent Voter Verifiable Records and the Innovation class;
- (2) Open Ended Vulnerability Testing; and
- (3) the usability and accessibility benchmarks developed for this iteration of the VVSG.

All three of these concepts are new to the VVSG and could have a substantial impact on the cost of implementation and on the security and accessibility of voting systems.

DATES: Comments must be received on or before 4 p.m. on March 5, 2008.

Submission of Comments: The EAC provides two means of submission of comments: (1) On-line electronic comment form at <http://www.eac.gov>, and (2) by mail to Voluntary Voting System Guidelines Comments, U.S. Election Assistance Commission, 1225 New York Ave., NW., Suite 1100, Washington, DC 20005. Commenters are encouraged to submit comments electronically to ensure timely receipt and consideration.

In order to allow efficient and effective review of comments the EAC requests that:

- (1) Comments should refer to the specific section that is the subject of the comment.
- (2) Comments regarding a term that is included or that should be added to the "Appendix A: Definitions of Words with Special Meanings" should reference the term, part, and section number to which the comment refers.
- (3) General comments regarding the entire document or comments that refer to more than one section should be made as specifically as possible so that EAC can clearly understand to which portion(s) of the documents the comment refers.
- (4) To the extent that a comment suggests a change in the wording of a

requirement or section of the guidelines, please provide proposed language for the suggested change.

To Obtain a copy of the TGDC Draft Recommendations of the Voluntary Voting System Guidelines: Due to the fact that the Voluntary Voting System Guidelines are more than 550 pages in length, the entire draft document has not been attached to this notice. A complete copy of the TGDC draft recommendations of the Voluntary Voting System Guidelines is available from the EAC in electronic format. An electronic copy can be downloaded in PDF format or read in HTML version on EAC's Web site, <http://www.eac.gov>. In order to obtain a paper copy of the TGDC draft recommendations please mail a written request to Voluntary Voting System Guidelines Comments, U.S. Election Assistance Commission, 1225 New York Ave., NW., Suite 1100, Washington, DC 20005.

FOR FURTHER INFORMATION CONTACT: Matthew Masterson, Phone (202) 566-3100, e-mail votingsystemstandards@eac.gov.

SUPPLEMENTARY INFORMATION: Prior to the passage of HAVA, the Federal Election Commission (FEC) published the 2002 Voting System Standards (VSS). HAVA mandated that the EAC update the VSS. In December of 2005 the EAC adopted the 2005 VVSG. The 2005 VVSG used many of the same requirements as the 2002 VSS but it expanded the security, accessibility, and usability sections. On March 29, 2006, the TGDC held its first meeting to discuss the next iteration of the VVSG. Since that time, the TGDC has held numerous public meetings and subcommittee conference calls to create a set of draft guidelines for recommendation to the EAC (all TGDC meeting materials can be found at <http://www.vote.nist.gov>). On August 17, 2007, the TGDC voted to complete final edits of their recommendations and submit them to the Executive Director of the EAC. The EAC received the draft guidelines from the TGDC on August 31, 2007.

The recommended guidelines currently consist of an Introduction and three distinct Parts. The Introduction is an overview of the requirements and explanations of new or expanded materials. Part 1 contains the equipment requirements including upgraded requirements for security and new usability benchmarks for voting machines. Part 2 details the documentation requirements for both the manufacturers and the Voting System Test Laboratories (VSTL). Part 2 also includes a section on the

submission of the Technical Data Package and requirements for full system user documentation. Part 3 contains the testing requirements for voting machines. This includes new material on open ended vulnerability testing and new benchmarks for performance testing. In addition to the introduction and the three parts, the guidelines contain (1) an appendix for "definitions of words with special meaning" specific to the requirements and (2) an appendix detailing all references and end notes.

Now that the TGDC has submitted its draft recommendations to the EAC for publication in the **Federal Register**, the EAC will begin its review and development process. This is a four phase plan:

Phase I—EAC will submit the TGDC's draft document to the **Federal Register** and provide a public comment feature on www.eac.gov. The public comment period will last for 120 days and all comments will be made available for public review. This public comment period is not required by law; however, the EAC thought it was extremely important to receive public input before proceeding with the process. During this public comment period the EAC will conduct public hearings regarding the TGDC's draft recommendations. The TGDC draft is currently available at <http://www.eac.gov>.

Phase II—EAC will collect and review all public comments submitted on the TGDC draft. After consideration of all public comments, the EAC will then perform an internal review.

Phase III—Based upon public comment and internal review of the TGDC document, the EAC will develop and publish its draft version in the **Federal Register**. The public will have another 120 days to comment on the EAC draft version. EAC will conduct public hearings to discuss its draft version.

Phase IV—EAC will collect and review all comments submitted and make final modifications. The final version of the VVSG will be adopted by vote of the Commission at a public meeting and then published in the **Federal Register**.

Thomas R. Wilkey,

Executive Director, U.S. Election Assistance Commission.

[FR Doc. 07-5526 Filed 11-5-07; 8:45 am]

BILLING CODE 6820-KF-M

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

Notice of Effectiveness of Exempt Wholesale Generator or Foreign Utility Company Status

October 26, 2007.

Benton County Wind Farm ...	EG07-64-000
Scurry County Wind L.P.	EG07-65-000
Jeffers Wind 20, LLC	EG07-66-000
Mansfield 2007 Trust A	EG07-67-000
Mansfield 2007 Trust B	EG07-68-000
Mansfield 2007 Trust C	EG07-69-000
Mansfield 2007 Trust D	EG07-70-000
Mansfield 2007 Trust E	EG07-71-000
Mansfield 2007 Trust F	EG07-72-000
Airtricity Munnsville Wind Farm, LLC	EG07-73-000
CPV Liberty, LLC	EG07-74-000
Gas Natural BAN, S.A.	FC07-52-000
Transportista Eléctrica Centroamericana, S.A.	FC07-53-000

Take notice that during the month of September 2007, the status of the above-captioned entities as Exempt Wholesale Generators or Foreign Utility Companies became effective by operation of the Commission's regulations, with the exception of EG07-65-000, which became effective in July 2007. 18 CFR 366.7(a).

Kimberly D. Bose,
Secretary.

[FR Doc. E7-21732 Filed 11-5-07; 8:45 am]

BILLING CODE 6717-01-P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Docket No. CP08-7-000]

Quicksilver Resources, Inc.; BreitBurn Operating L.P.; Notice of Petition for Declaratory Order

October 26, 2007.

Take notice that on October 5, 2007, Quicksilver Resources, Inc. and BreitBurn Operating L.P. (collectively Petitioners), under Rule 207(a)(2) of the Commission's Rules of Practice and Procedure, 18 CFR 385.207(a)(2) (2007), filed a petition for a declaratory order requesting that the Commission disclaim jurisdiction over certain natural gas facilities because such facilities perform a gathering function exempt from the Commission's jurisdiction under section 1(b) of the Natural Gas Act.

Any person desiring to intervene or to protest this filing must file in accordance with Rules 211 and 214 of



U.S. ELECTION ASSISTANCE COMMISSION
1201 NEW YORK AVENUE, N.W., SUITE 300
WASHINGTON, D.C. 20005

OFFICE OF THE CHAIR

BEFORE THE ELECTION ASSISTANCE COMMISSION

In the Matter of)
)
Submission of UOCAVA Pilot Program Testing)
Requirements for Public Notice and Comment)
)
)
)

CERTIFICATION

I, Donetta Davidson, Chair of the Election Assistance Commission, do hereby certify that on March 30, 2010 the Commission decided by a vote of 3-0. The following action(s) were taken:

1.

The Commission should approve posting the "UOCAVA Pilot Program Testing Requirements" for a 30-day public comment period pursuant to the EAC's current "Notice and Public Comment Policy." This document has been e-mailed to you for your review (approximately 100 pages).

Commissioners Beach, Davidson, and Hillman approved the recommendation.

Attest:

3-30-10
Date

Donetta Davidson
Donetta Davidson
Chair



U.S. ELECTION ASSISTANCE COMMISSION
1225 New York Ave. NW - Suite 1100
Washington, DC 20005

MEMORANDUM

TO: Commissioner Beach, Commissioner Hillman

FROM: Commissioner Donetta Davidson *Donetta Davidson*

DATE: March 26, 2010

RE: Submission of UOCAVA Pilot Program Testing Requirements for Public Notice and Comment

The current Voluntary Voting System Guidelines contain standards for traditional voting machine types, such as optical scan and direct record electronic machines. Many States are currently exploring the possibility of implementing new technologies to better serve UOCAVA voters.

In order for EAC to provide a process for these States to have their systems tested, EAC, in conjunction with NIST, have created proposed requirements for EAC testing of voting systems to be used in pilot projects for UOCAVA voters. In addition, this set of testable requirements, when completed, will be turned over to the Technical Guidelines Development Committee to aid their work in developing a full set of guidelines for PC-based remote electronic voting, as required by the 2005 Defense Authorization Act.

To give the general public ample time to consider the requirements, this document has already been posted to EAC's Website

RECOMMENDATION:

Approve posting the "UOCAVA Pilot Program Testing Requirements" for a 30-day public comment period pursuant to the EAC's current "Notice and Public Comment Policy." This document has been emailed to you for your review (approximately 100 pages).



U.S. ELECTION ASSISTANCE COMMISSION
1225 New York Ave. NW - Suite 1100
Washington, DC 20005

TALLY VOTE MATTER

DATE & TIME OF TRANSMITTAL: March 26, 2010, 6:00 p.m.

BALLOT DEADLINE: March 30, 2010, 6:00 p.m.

COMMISSIONERS: BEACH, DAVIDSON, AND HILLMAN

SUBJECT: SUBMISSION OF UOCAVA PILOT PROGRAM TESTING
REQUIREMENTS FOR PUBLIC NOTICE AND COMMENT

- () I approve the recommendation.
- () I disapprove the recommendation.
- () I object to the recommendation.
- () I am recused from voting.

COMMENTS: _____

DATE: _____ SIGNATURE: _____

A definite vote is required. All ballots must be signed and dated. Please return ONLY THE BALLOT to the EAC Chair. Please return the ballot no later than date and time shown above.

FROM DONETTA DAVIDSON, CHAIR



U.S. ELECTION ASSISTANCE COMMISSION
1225 New York Ave. NW - Suite 1100
Washington, DC 20005

TALLY VOTE MATTER

DATE & TIME OF TRANSMITTAL: March 26, 2010, 6:00 p.m.

BALLOT DEADLINE: March 30, 2010, 6:00 p.m.

COMMISSIONERS: BEACH, DAVIDSON, AND HILLMAN

SUBJECT: SUBMISSION OF UOCAVA PILOT PROGRAM TESTING REQUIREMENTS FOR PUBLIC NOTICE AND COMMENT

- I approve the recommendation.
- I disapprove the recommendation.
- I object to the recommendation.
- I am recused from voting.

COMMENTS: _____

DATE: 3-26-10 **SIGNATURE:** Donetta Davidson

A definite vote is required. All ballots must be signed and dated. Please return ONLY THE BALLOT to the EAC Chair. Please return the ballot no later than date and time shown above.

FROM DONETTA DAVIDSON, CHAIR



U.S. ELECTION ASSISTANCE COMMISSION
1225 New York Ave. NW - Suite 1100
Washington, DC 20005

TALLY VOTE MATTER

DATE & TIME OF TRANSMITTAL: March 26, 2010, 6:00 p.m.

BALLOT DEADLINE: March 30, 2010, 6:00 p.m.

COMMISSIONERS: BEACH, DAVIDSON, AND HILLMAN

SUBJECT: SUBMISSION OF UOCAVA PILOT PROGRAM TESTING REQUIREMENTS FOR PUBLIC NOTICE AND COMMENT

- I approve the recommendation.
- I disapprove the recommendation.
- I object to the recommendation.
- I am recused from voting.

COMMENTS: _____

DATE: 3/29/10 **SIGNATURE:** Ames Beach

A definite vote is required. All ballots must be signed and dated. Please return ONLY THE BALLOT to the EAC Chair. Please return the ballot no later than date and time shown above.

FROM DONETTA DAVIDSON, CHAIR



U.S. ELECTION ASSISTANCE COMMISSION
1225 New York Ave. NW - Suite 1100
Washington, DC 20005

TALLY VOTE MATTER

DATE & TIME OF TRANSMITTAL: March 26, 2010, 6:00 p.m.

BALLOT DEADLINE: March 30, 2010, 6:00 p.m.

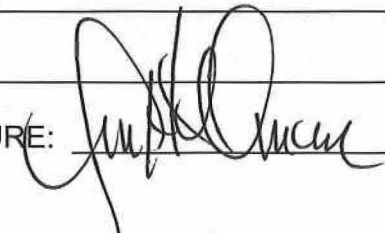
COMMISSIONERS: BEACH, DAVIDSON, AND HILLMAN

SUBJECT: SUBMISSION OF UOCAVA PILOT PROGRAM TESTING REQUIREMENTS FOR PUBLIC NOTICE AND COMMENT

- I approve the recommendation.
- I disapprove the recommendation.
- I object to the recommendation.
- I am recused from voting.

COMMENTS: _____

DATE: 3-29-10

SIGNATURE: 

A definite vote is required. All ballots must be signed and dated. Please return ONLY THE BALLOT to the EAC Chair. Please return the ballot no later than date and time shown above.

FROM DONETTA DAVIDSON, CHAIR