United States Government Accountability Office

GAO

Report to the Chairwoman, Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, House of Representatives

September 2010

INFORMATION SECURITY

Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems

GAO-10-916

September 2010

INFORMATION SECURITY

Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-916, a report to the Chairwoman, Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Historically, civilian and national security-related information technology (IT) systems have been governed by different information security policies and guidance. Specifically, the Office of Management and Budget and the Department of Commerce's National Institute of Standards and Technology (NIST) established policies and guidance for civilian non-national security systems, while other organizations, including the Committee on National Security Systems (CNSS), the Department of Defense (DOD), and the U.S. intelligence community, have developed policies and guidance for national security systems.

GAO was asked to assess the progress of federal efforts to harmonize policies and guidance for these two types of systems. To do this, GAO reviewed program plans and schedules, analyzed policies and guidance, assessed program efforts against key practices for cross-agency collaboration, and interviewed officials responsible for this effort.

What GAO Recommends

GAO is recommending that the Secretary of Commerce and the Secretary of Defense, among other things, update plans for future collaboration, establish timelines for implementing revised guidance, and fully implement key practices for interagency collaboration in the harmonization effort. In comments on a draft of this report, Commerce and DOD concurred with GAO's recommendations.

View GAO-10-916 or key components.
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Federal agencies have made progress in harmonizing information security policies and guidance for national security and non-national security systems. Representatives from civilian, defense, and intelligence agencies established a joint task force in 2009, led by NIST and including senior leadership and subject matter experts from participating agencies, to publish common guidance for information systems security for national security and non-national security systems. The harmonized guidance is to consist of NIST guidance applicable to non-national security systems and authorized by CNSS, with possible modifications, for application to national security systems. This harmonized security guidance is expected to result in less duplication of effort and more effective implementation of controls across multiple interconnected systems. The task force has developed three initial publications. These publications, among other things, provide guidance for applying a risk management framework to federal systems, identify an updated catalog of security controls and guidelines, and update the existing security assessment guidelines for federal systems. CNSS has issued an instruction to begin implementing the newly developed guidance for national security systems. Two additional joint publications are scheduled for release by early 2011, with other publications under consideration. Differences remain between guidance for national security and non-national security systems in such areas as system categorization, selection of security controls, and program management controls. NIST and CNSS officials stated that these differences may be addressed in the future but that some may remain because of the special nature of national security systems.

While progress has been made in developing the harmonized guidance, additional work remains to implement it and ensure continued progress. For example, task force members have stated their intent to develop plans for future harmonization activities, but these plans have not yet been finalized. In addition, while much of the harmonized guidance incorporates controls and language previously developed for use for non-national security systems, significant work remains to implement the guidance for national security systems. DOD and the intelligence community are developing agency-specific guidance and transition plans for implementing the harmonized guidance, but, according to officials, actual implementation could take several years to complete. Officials stated that this is primarily due to both the large number and criticality of the systems that must be reauthorized under the new guidance. Further, the agencies have yet to fully establish implementation milestones and lack performance metrics for measuring progress. Finally, the harmonization effort has been managed without full implementation of key collaborative practices, such as documenting identified needs and leveraging resources to address those needs, agreed-to agency roles and responsibilities, and processes to monitor and report results. Task force members stress that their informal, flexible approach has resulted in significant success. Nevertheless, further implementation of key collaborative practices identified by GAO could facilitate further progress.

Contents

Abbreviations

CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CNSSI-1253	Committee on National Security Systems Instruction 1253
DCID	Director Central Intelligence Directive
DIACAP	DOD Information Assurance Certification and Accreditation Process
DOD	Department of Defense
DODI	Department of Defense Instruction
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
NIST	National Institute of Standards and Technology
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 15, 2010

The Honorable Diane Watson
Chairwoman
Subcommittee on Government Management,
Organization, and Procurement
Committee on Oversight and Government Reform
House of Representatives

Dear Chairwoman Watson:

Historically, civilian and national security-related information technology (IT) systems have been governed by different information security policies and guidance. However, over time, factors such as the increasing interconnectedness of computer systems have led to these systems facing similar threats.

Development of a unified information security framework that harmonizes security standards and guidance for national security systems and non-national security systems has been highlighted as having the potential to improve information security and avoid unnecessary and costly duplication of effort. As agreed with your office, our objective was to assess the progress of federal efforts to harmonize policies and guidance for national security systems and non-national security systems.

To identify efforts to harmonize policies and guidance for national security systems and non-national security systems, we identified completed and planned efforts by the Department of Commerce's National Institute of Standards and Technology (NIST), Department of Defense (DOD), Committee on National Security Systems (CNSS), and the Office of the Director of National Intelligence (ODNI) to issue joint information security policies and guidance. We then reviewed related publications, guidance, plans, and other documents from these organizations to identify differences in existing guidance and plans to resolve those differences and conducted interviews with officials to discuss these differences, the status of harmonization efforts, and the implications for the security of information systems. We also evaluated completed and planned activities against criteria including prior GAO work on key practices to enhance and sustain cross-agency collaboration. Appendix I contains additional details on the objective, scope, and methodology of our review.

We conducted this performance audit from February 2010 to September 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 objective.

Background

The Federal Information Security Management Act (FISMA) specifies requirements for protecting federal systems and data. Enacted into law on December 17, 2002, as title III of the E-Government Act of 2002, FISMA requires every federal agency, including agencies with national security systems,[1] to develop, document, and implement an agencywide information security program to secure 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. Specifically, this program is to include

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices that include testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;

[1]As defined in FISMA, the term "national security system" means any information system used by or on behalf of a federal agency that (1) involves intelligence activities, national security-related cryptologic activities, command and control of military forces, or equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions (excluding systems used for routine administrative and business applications) or (2) is protected at all times by procedures established for handling classified national security information. See 44 U.S.C. § 3542(b)(2). For the purposes of this report, systems that do not meet the criteria for national security systems are referred to as non-national security systems.

- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

FISMA also assigns specific information security responsibilities to the Office of Management and Budget (OMB), NIST, agency heads, and agency chief information officers (CIO). Generally, OMB is responsible for developing policies and guidance and overseeing agency compliance with FISMA, NIST is responsible for developing technical standards, and agency heads and CIOs are responsible for ensuring that each agency implements the information security program and other requirements of FISMA.

These responsibilities do not, however, apply equally to all agency information systems. FISMA differs in its treatment of national security and non-national security systems. While FISMA requires each federal agency to manage its information security risks through its agencywide information security program, the law recognizes a long-standing division between requirements for national security and non-national security

systems that limits civilian management and oversight of information systems supporting military and intelligence activities.[2]

FISMA recognizes the division between national security systems and non-national security systems in two ways. First, to ensure compliance with applicable authorities, the law requires agencies using national security systems to implement information security policies and practices as required by standards and guidelines for national security systems in addition to the requirements of FISMA. Second, the responsibilities assigned by FISMA to OMB and NIST are curtailed. OMB's responsibilities are reduced with regard to national security systems to oversight and reporting to Congress on agency compliance with FISMA. OMB's annual review and approval or disapproval of agency information security programs, for example, does not include national security systems.[3] Similarly, according to FISMA, NIST-developed standards, which are mandatory for non-national security systems, do not apply to national security systems. FISMA limits NIST to developing, in conjunction with DOD and the National Security Agency (NSA), guidelines for agencies on identifying an information system as a national security system, and for ensuring that NIST standards and guidelines are complementary with standards and guidelines developed for national security systems. FISMA also requires NIST to consult with other agencies to ensure use of appropriate information security policies, procedures, and techniques in

[2]The differing treatment of national security and non-national security systems reflects a long-standing division in laws that limit civilian management oversight of military and intelligence information systems by excluding national security systems from the "information technology" overseen by the civilian agencies. OMB authority over such systems is limited in FISMA (44 U.S.C. § 3543(b)), in the Paperwork Reduction Act (44 U.S.C. § 3502(9)), and in the Clinger-Cohen Act (40 U.S.C. § 11103). NIST authority is limited by 15 U.S.C. § 278g-3(a)(2), as amended by FISMA, but also under the prior language of the Computer Security Act of 1987 (Pub. L. 100-235, Jan. 8, 1988). These limitations are variations of a provision, known as the "Warner Amendment," added to the DOD Authorization Act of 1982, which exempted DOD procurement of national security systems from General Services Administration oversight under the Brooks Act (then-40 U.S.C. § 759). Pub. L. 97-86, title IX, § 908(a)(1), Dec. 1, 1981; 10 U.S.C. § 2315.

[3]In addition to placing limitations on OMB's authority over national security systems, FISMA permits further independence from OMB oversight for Department of Defense and Central Intelligence Agency systems where loss of security would have a debilitating impact on the mission of either agency, 44 U.S.C. 3543(c). More generally, FISMA also states that it does not affect authorities otherwise granted an agency with regard to national security systems (as well as requirements under the Atomic Energy Act of 1954), Sec. 301(c), Pub. L. 107-347 (116 Stat. 2955); 44 U.S.C. 3501 note.

order to improve information security and avoid unnecessary and costly duplication of effort.

In light of this division between national security and non-national security systems, NIST is responsible for developing standards and guidance for non-national security information systems. For example, NIST issues mandatory Federal Information Processing Standards (FIPS) and special publications that provide guidance for information systems security for non-national security systems in federal agencies.

For national security systems, National Security Directive 42 established CNSS, an organization chaired by the Department of Defense, to, among other things, issue policy directives and instructions that provide mandatory information security requirements for national security systems.[4] In addition, the defense and intelligence communities develop implementing instructions and may add additional requirements where needed.

FISMA provides a further exception to compliance with NIST standards. It permits an agency to use more stringent information security standards if it certifies that its standards are at least as stringent as the NIST standards and are otherwise consistent with policies and guidelines issued under FISMA. It is on the basis of this authority that the Department of Defense establishes information security standards for all of its systems (national security and non-national security systems) that are more stringent than the standards required for protecting non-national security systems under FISMA. For example, the DOD directive establishing the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) for authorizing the operation of DOD information systems requires annual certification that the DIACAP process is current and more stringent than NIST standards under FISMA.

NIST Guidance Provides Basic Framework for Security of Non-National Security Systems

To help implement the provisions of FISMA for non-national security systems, NIST has developed a risk management framework for agencies to follow in developing information security programs. The framework is specified in NIST Special Publication (SP) 800-37, revision 1, *Guide for Applying the Risk Management Framework to Federal Information*

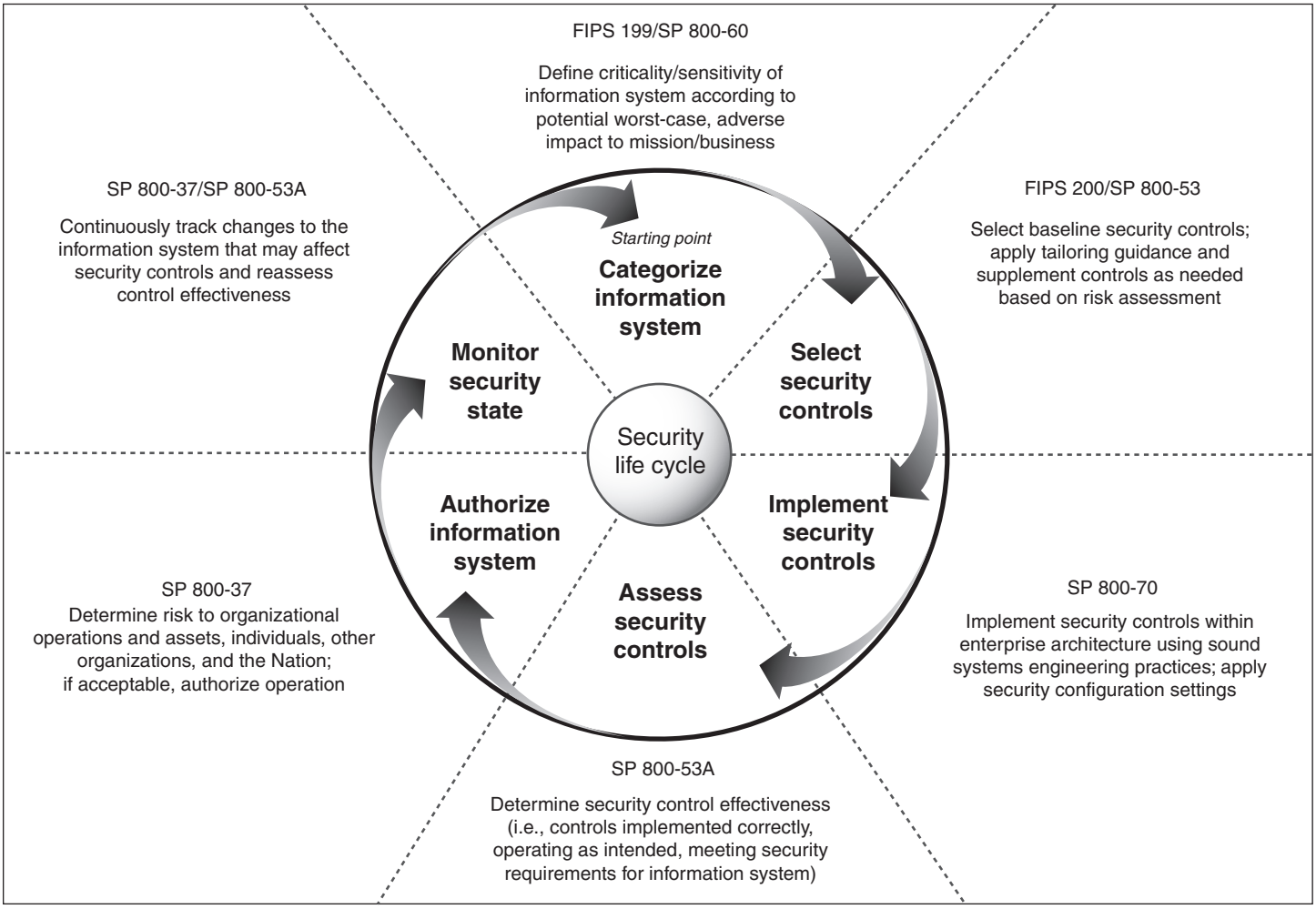
[4]National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, July 5, 1990.

Systems: A Security Life Cycle Approach,[5] which provides agencies with guidance for applying the risk management framework to federal information systems.[6] The framework in SP 800-37 consists of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. It also provides a process that integrates information security and risk management activities into the system development life cycle. Figure 1 provides an illustration of the framework and notes relevant security guidance for each part of the framework.

[5]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems*, SP 800-37, revision 1 (Gaithersburg, Md.: February 2010).

[6]NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems*, SP 800-37, revision 1, was formerly NIST, *Guide for the Certification and Accreditation of Federal Information Systems*, SP 800-37. The risk management framework replaces the process known as certification and accreditation described in the previous version of SP 800-37.

Figure 1: NIST Risk Management Framework



Source: GAO analysis of NIST data.

Other key NIST publications related to the risk management framework include the following:

- Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*.[7] Provides agencies with criteria to identify and categorize their

[7]NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, Md.: February 2004).

information systems based on providing appropriate levels of information security according to a range of risk levels.

- NIST SP 800-60, revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*.[8] Provides guidance for implementing FIPS 199.

- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.[9] Provides minimum information security requirements for protecting the confidentiality, integrity, and availability of federal information systems.

- NIST SP 800-53 revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*.[10] Provides guidelines for selecting and specifying security controls for information systems.

- NIST SP 800-70, revision 1, *National Checklist Program for IT Products-Guidelines for Checklist Users and Developers*.[11] Provides guidance for using the National Checklist Repository to select a security configuration checklist, which may include items such as security controls used in FISMA system assessments.[12]

- NIST SP 800-53A, revision 1, *Guide for Assessing the Security Controls in Federal Information Systems*.[13] Provides agencies with guidance for building security assessment plans and procedures for assessing the effectiveness of security controls employed in information systems.

[8]NIST, *Guide for Mapping Types of Information and Information Systems to Security Categories*, SP 800-60, revision 1 (Gaithersburg, Md.: August 2008).

[9]NIST, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS Publication 200 (Gaithersburg, Md.: March 2006).

[10]NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, SP 800-53, revision 3 (Gaithersburg, Md.: August 2009).

[11]NIST, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, SP 800-70, revision 1 (Gaithersburg, Md.: September 2009).

[12]NIST maintains the National Checklist Repository, which is a publicly available resource that contains a variety of security configuration checklists for specific IT products or categories of IT products.

[13]NIST, *Guide for Assessing the Security Controls in Federal Information Systems*, SP 800-53A (Gaithersburg, Md.: June 2010).

In applying the provisions of FIPS 200, federal civilian agencies with non-national security systems are to first categorize their information and systems as required by FIPS 199, and then should select an appropriate set of security controls from NIST SP 800-53 to satisfy their minimum security requirements. This helps to ensure that appropriate security requirements and security controls are applied to all non-national security systems. Next, controls are implemented and information systems are authorized using NIST SP 800-70. Finally, agencies assess, test, and monitor the effectiveness of the information security controls using the guidance in NIST SP 800-53A. Many other FIPS and NIST special publications provide guidance for the implementation of FISMA requirements for non-national security systems.

CNSS Provides the Basic Security Framework for National Security Systems with Defense and Intelligence Agencies Providing Additional Guidance

For national security systems, organizations responsible for developing policies, directives, and guidance include CNSS, DOD, and the intelligence community. The processes and criteria established by this guidance are often similar to those required by NIST guidance for non-national security systems. For example, security guidance for certification and accreditation requires risk assessments, verification of security requirements in a security plan or other document, testing of security controls, and formal authorization by an authorizing official. Roles of these agencies and key security guidance that they have issued are described below.

Committee on National Security Systems

CNSS provides a forum for the discussion of policy issues, sets national policy, and provides direction, operational procedures, and guidance for the security of national security systems. The Department of Defense chairs the committee under the authorities established by National Security Directive 42, issued in July 1990.[14] This directive designates the Secretary of Defense and the Director of the National Security Agency as the Executive Agent and National Manager for national security systems, respectively.

[14]National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, July 5, 1990.

The committee has voting representatives from 21 departments and agencies.[15] In addition, nonvoting observers such as NIST participate in meetings, provide comments and suggestions, and participate in subcommittee and working group activities. The committee organizes its activities by developing an annual program of work and plan of action and milestones. NSA provides logistical and administrative support for the committee, including a Secretariat manager who organizes the day-to-day activities of the committee.

Since its inception, the committee has issued numerous policies, directives, and instructions that are binding upon all federal departments and agencies for national security systems. Key publications include the *Information Assurance Risk Management Policy for National Security Systems*,[16] *National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems*,[17] *National Information Assurance Certification and Accreditation Process*,[18] and a *National Information Assurance Glossary*.[19]

Department of Defense

To defend DOD information systems and computer networks from unauthorized or malicious activity, the department established an Information Assurance Framework in its 8500 series of guidance. This framework allows DOD to ensure the security of its information systems by providing standards and support to its component information assurance programs. DOD uses this framework for all of its IT systems. DOD directive 8500.01 and implementing instruction 8500.2, which documents information security controls, are the primary policy

[15]The departments and agencies with voting representatives are the Departments of Commerce, Defense, Energy, Homeland Security, Justice, State, Transportation, and the Treasury; the Central Intelligence Agency; the Defense Intelligence Agency; the Federal Bureau of Investigation; the General Services Administration; the National Security Agency; the National Security Council; the Office of the Director of National Intelligence; the Office of Management and Budget; the Joint Chiefs of Staff; the Air Force; the Army; the Marine Corps; and the Navy.

[16]CNSS Policy 22, *Information Assurance Risk Management Policy for National Security Systems*, February 2009.

[17]CNSS Policy 6, *National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems*, October 2005.

[18]National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, July 5, 1990.

[19]CNSS Instruction 4009 (CNSSI 4009), *National Information Assurance Glossary*, June 2006.

documents that describe this framework. In addition, the Department of Defense Information Assurance Certification and Accreditation Process, published in November 2007, is documented in DOD 8510.01 and the online DIACAP knowledge service. Also, the establishment of an information security program is described in DOD regulation 5200.01-R, dated January 1997.

Intelligence Community

The intelligence community is a federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States.[20] Member organizations include intelligence agencies, military intelligence, and civilian intelligence and analysis offices within federal executive departments. The community is led by the Director of National Intelligence, who oversees and directs the implementation of the National Intelligence Program.

Historically, the intelligence community has had separate instructions related to information system security. For example, Director of Central Intelligence Directive (DCID) 6/3, *Protecting Sensitive Compartmented Information within Information Systems*,[21] and its implementation manual provided policy and procedures for the security and protection of systems that create, process, store, and transmit intelligence information, and defined and mandated the use of a risk management process and a certification and accreditation process.

[20]The organizations are the Central Intelligence Agency, Defense Intelligence Agency, Department of Energy (Office of Intelligence and Counterintelligence), Department of Homeland Security (Office of Intelligence and Analysis), Department of State (Bureau of Intelligence and Research), Department of the Treasury (Office of Intelligence and Analysis), Drug Enforcement Administration (Office of National Security Intelligence), Federal Bureau of Investigation (National Security Branch), National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency/Central Security Service, United States Air Force, United States Army, United States Coast Guard, United States Marine Corps, United States Navy, and Office of the Director of National Intelligence.

[21]Director of Central Intelligence Directive 6/3, *Protecting Sensitive Compartmented Information within Information Systems—Policy*, June 5, 1999.

Federal Agencies Have Had Disparate Information Security Guidance

Prior to efforts to harmonize information security guidance, federal organizations had developed separate, and sometimes disparate, guidance for information security. For example, the National Security Agency used the National Information Systems Certification and Accreditation Process, the intelligence community used DCID 6/3, and DOD used the Department of Defense Information Technology Security Certification and Accreditation Process, which later became the DIACAP.

According to the Federal CIO Council's strategic plan and federal officials in DOD and the intelligence community, these processes had some elements in common;[22] however, the variances in guidance were sufficient to cause several unintended and undesirable consequences for the federal community. For example, both DOD and NIST had catalogs of information security controls that covered similar areas but had different formats and structures.

As a result, according to the CIO Council, organizations responsible for providing oversight of federal information systems such as members of the CIO Council and CNSS could not easily assess the security of federal information systems. In addition, reciprocity—the mutual agreement among participating enterprises to accept each other's security assessments—was hampered because of the apparent differences in interpreting risk levels. Because agencies were not confident in their understanding of other agencies' certification and accreditation results, they sometimes felt it necessary to recertify and reaccredit information systems, expending resources, including time and money, which may not have been necessary.[23]

Progress Is Being Made to Harmonize IT Security Guidance

A task force consisting of representatives from civilian, defense, and intelligence agencies has made progress in establishing a unified information security framework for national security and non-national security systems. Specifically, NIST has published three initial documents developed by a task force working group to harmonize information security standards for national security and non-national security systems,

[22]The Federal CIO Council is an interagency forum for improving agency IT practices. The council, chaired by OMB, coordinates with NIST and CNSS on the development of harmonized information system guidance.

[23]*Federal Information Management Strategic Plan*, *Federal Chief Information Officers Council Framework* (Fiscal Years 2010–2013), January 26, 2010.

and is scheduled to publish two more by early 2011. While much has been accomplished, differences remain between the guidance for the two types of systems, and significant work remains to implement the harmonized guidance on national security systems, such as developing supporting agency-specific guidance and establishing specific time frames and performance measures for implementation. Further, while the task force has implemented elements of key practices for interagency coordination that GAO has identified, much of this implementation is not documented. The lack of fully implemented practices, such as those that assign responsibilities and measure progress, could limit the task force's continued progress as personnel change and resources are allocated among other agency activities.

A Joint Task Force Has Been Established to Create a Unified Information Security Framework

According to NIST and CNSS officials, a Joint Task Force Transformation Initiative Interagency Working Group was formed in April 2009 with representatives from NIST, DOD, and ODNI to produce a unified information security framework for the federal government. Instead of having parallel publications for national security systems and non-national security systems for risk management and systems security, the intent, according to members of the joint task force, is to have common publications to the maximum extent possible. According to officials involved in the task force, harmonized security guidance is expected to result in less duplication of effort, lower maintenance costs, and more effective implementation of controls across multiple interconnected systems. In addition, the harmonized guidance should make it simpler and more cost-effective for vendors and contractors to supply security products and services to the federal government.

The task force arose out of prior efforts to harmonize security guidance among national security systems. In 2006, the ODNI and DOD CIOs began an initiative to harmonize the two organizations' certification and accreditation guidance and processes for IT systems. For example, in July 2006, DOD and the intelligence community established a Unified Cross Domain Management Office to address duplication and uncoordinated security activities and improve the security posture of the agencies' highest-risk security devices. In January 2007, the DOD and ODNI CIOs published seven certification and accreditation transformation goals that included development of common security controls. According to DOD, by July 2008, DOD and the intelligence community were working on six documents that mirrored similar NIST risk management and information security publications. In August 2008, the CIOs signed an agreement

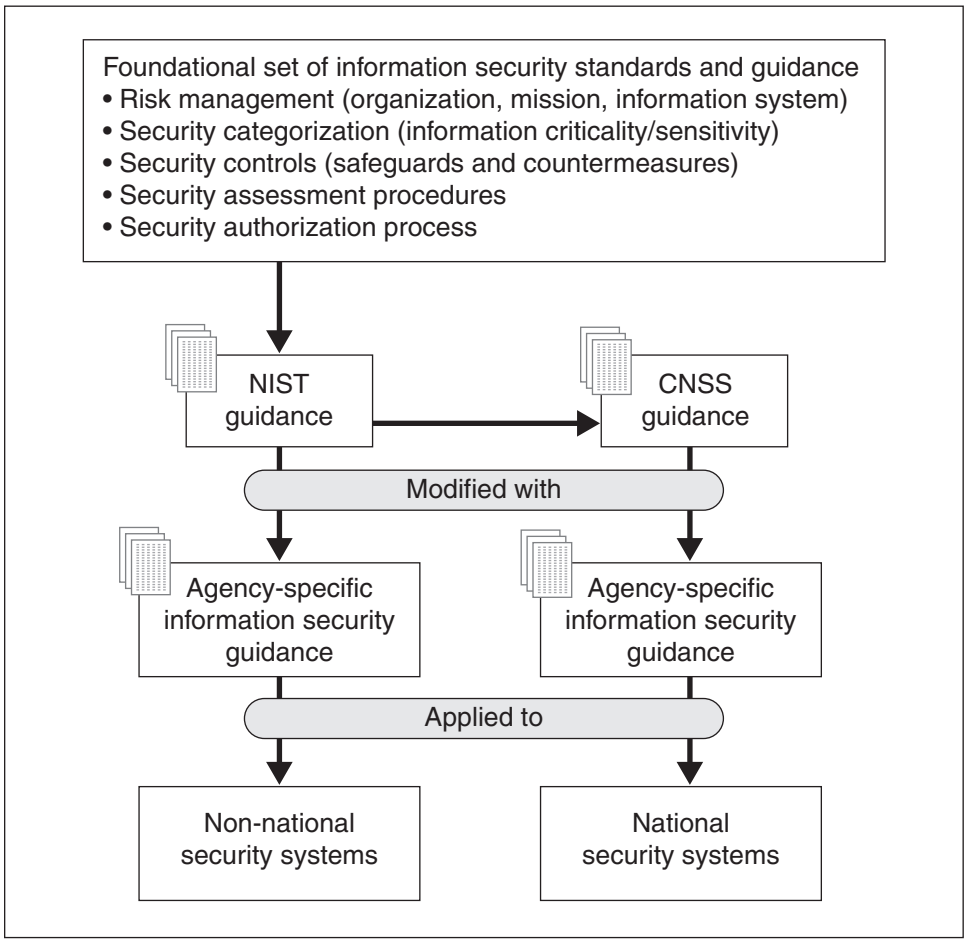
adopting common guidelines to streamline and build reciprocity into the certification and accreditation process.

As this effort progressed, the agencies involved determined that it would benefit from closer engagement with NIST and the development of common security guidance. NIST had been informally involved in the harmonization effort for several years, but, according to CNSS, DOD, and ODNI, during the CNSS annual conference in the spring of 2009, the CNSS community decided to more actively engage NIST and agree to use NIST documents as the basis for information security controls and risk management. The committee also agreed to complete policies and instructions to support use of the NIST publications. Following the conference, a memo from the Acting CIO for the intelligence community stated that the intelligence community intended to follow CNSS guidance that pointed to related NIST publications.

NIST currently leads the working group and the task force publication development process. Working group members are selected for each publication from participating agencies and support contractors to provide subject matter expertise and administrative support. In addition, the task force is guided by a senior leadership team from NIST, CNSS, DOD, and ODNI that reviews and approves the harmonized publications.

As illustrated in figure 2, key areas targeted for the common guidance include risk management, security categorization, security controls, security assessment procedures, and the security authorization process contained in the NIST risk management framework. NIST develops standards and guidance for non-national security systems, including most systems in civilian agencies. CNSS provides policy, directives, and instructions binding upon all U.S. government departments and agencies for national security systems, including systems in the intelligence community and DOD (e.g., classified systems). Since NIST does not have authority over national security systems, CNSS issuances authorize the use of the harmonized NIST guidance developed by the joint task force. As necessary, CNSS also develops additional information security requirements to accommodate the unique nature of national security systems. Finally, individual agencies may create their own specific implementing guidance.

Figure 2: Unified Information Security Framework



Sources: NIST and CNSS.

Note: The foundational set of common information security requirements links to the requirements in the NIST Risk Management Framework.

Joint Task Force Has Published Three Initial Harmonized Guidance Publications

The joint task force has published three of five planned publications containing harmonized information security guidance and is actively developing the final two publications. These include a new publication as well as revisions to existing NIST guidance, as summarized in table 1. In addition, the task force is considering collaboration on two additional publications.

Table 1: Joint Task Force Completed and Planned Publications

Publication	Issue date
NIST SP 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	August 2009
NIST SP 800-37, revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*	February 2010
NIST SP 800-53A, revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*	June 2010
NIST SP 800-39*, Enterprise-Wide Risk Management: Organization, Mission, and Information Systems View*	January 2011 (planned)
NIST SP 800-30, revision 1, *Guide for Conducting Risk Assessments*	February 2011 (planned)

Source: NIST.

As of June 2010, the three publications developed by the joint task force and released by NIST are the following:

- NIST SP 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, was published in August 2009. It contains the catalog of security controls and technical guidelines that federal agencies will use to protect federal information and information systems, and is an integral part of the unified information security framework for the entire federal government. The security controls within revision 3 provide updated security controls developed by the joint task force members that included NIST, CNSS, DOD, and ODNI with specific information from databases of known cyber attacks and threat information. According to the task force leader and the CNSS manager, new controls and enhancements were added as a result of the harmonization effort. For example, control AC-4, related to Information Flow Enforcement, had several enhancements added because of input from the national security systems community.

- NIST SP 800-37, revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, was released in February 2010. This publication replaces the traditional certification and accreditation process with the six-step risk management framework, including a process of assessment and authorization. [24] According to the publication, the revised process emphasizes building information security capabilities into federal information systems through the application of security controls while

[24]The assessment and authorization process replaces the process known as certification and accreditation described in the previous version of SP 800-37.

implementing an ongoing monitoring process. It also provides information to senior leaders to facilitate better decisions regarding the acceptance of risk arising from the operation and use of information systems. According to the task force leader and the CNSS manager, the publication contains few direct changes as a result of the harmonization effort. Rather, task force representatives determined that the existing NIST risk management framework contained the same concepts and content as existing national security-related guidance, such as the DIACAP.

- NIST SP 800-53A, revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, was published in June 2010. The updated security assessment guideline is intended to incorporate leading practices in information security from DOD, the intelligence community, and civil agencies and includes security control assessment procedures for both national security and non-national security systems. The guidelines for developing security assessment plans are intended to support a wide variety of assessment activities in all phases of the system development life cycle, including development, implementation, and operation. According to the task force leader and the CNSS manager, while there were few direct changes to the content of SP 800-53A as a result of the harmonization effort, task force members are collaborating on revising the assessment cases, which provide additional instruction on techniques for testing specific controls. According to the leader, this effort is to be completed by the end of 2010.

  Because CNSS, not NIST, has the authority to issue binding guidance for national security systems, CNSS has issued supplemental guidance for implementing NIST SP 800-53: CNSS Instruction 1253 (CNSSI-1253), *Security Categorization and Control Selection for National Security Systems*, which was published in October 2009. This instruction states that the Director of National Intelligence and the Secretary of Defense have directed that the processes described in NIST SP 800-53, revision 3 (as amended by the instruction), and the NIST security and programmatic controls contained in 800-53 apply to national security systems. Using the controls in 800-53, this instruction provides categorization and corresponding baseline sets of controls for national security systems.

  CNSS also recently published a revised common glossary of information security terms in support of the goal of adopting a common lexicon for the national security and non-national security communities.[25] This revised

[25]CNSS Instruction 4009, *National Information Assurance (IA) Glossary*, April 26, 2010.

glossary harmonizes terminology used by DOD, the intelligence community, and civil agencies (which use a NIST-developed glossary) to enable all three to use the same terminology (and move toward shared documentation and processes).

According to the CNSS Secretariat manager, in December 2010 CNSS plans to revise an existing policy, CNSSP 6, to generally direct the use of NIST publications, including SP 800-37 and SP 800-53A, as common guidance and will include related CNSS instructions (if any) on how to implement the NIST guidance for national security systems.[26] This will coincide closely with the publication of NIST SP 800-39 and SP 800-30, revision 1. The CNSS manager stated that once common guidance developed jointly with NIST is finalized, CNSS needs to determine whether it will need supplemental instructions because of the uniqueness of national security systems (e.g., their special operating environments or the classified information they contain). However, CNSS officials said that the committee intends to keep this unique guidance to a minimum and use the common security guidance to the maximum extent possible.

The joint task force's development schedule lists two additional joint task force publications:

- NIST SP 800-39, *Enterprise-Wide Risk Management: Organization, Mission, and Information Systems View*, planned for publication in January 2011, is to provide an approach for managing that portion of risk resulting from the incorporation of information systems into the mission and business processes of an organization.

- NIST SP 800-30, revision 1, *Guide for Conducting Risk Assessments*, planned for publication in February 2011, is a revision of an existing NIST publication that will be refocused to address risk assessments as part of the risk management framework.

In addition to the two planned publications, the joint task force leader and the CNSS Secretariat manager stated that two other publications are under consideration for collaboration:

- *Guide for Information System Security Engineering*, under consideration for publication in September 2011, and

[26]CNSS Policy 6, *National Policy on Certification and Accreditation of National Security Systems*, October 2005.

- *Guide for Software Application Security*, under consideration for publication in November 2011.

The estimated completion dates for these future publications are later than originally planned. For example, as of January 2010, SP 800-39 and SP 800-30, revision 1, were to have been completed in August 2010, and the information system security engineering guide was to be completed in October 2010. According to the task force leader, the delays are due to additional work and coordination activities that needed to be completed, the breadth and depth of comments in the review process, and challenges in coordination with other task force members.

Task force members acknowledge that there are additional areas of IT security guidance where it may be possible to collaborate, but they have not yet documented plans for future efforts. The CNSS manager stated that the committee intends to update its existing plan of action and milestones in fall 2010, but this has not yet been completed. Until the task force defines topics and deadlines for future efforts, opportunities for additional collaboration will likely be constrained.

Differences Remain between Guidance for National Security Systems and Non-National Security Systems

Despite the efforts to harmonize information security guidance, many differences remain. These include differences in system categorization, selection of security controls, and use of program management controls.

System categorization. Different methodologies are used to categorize the impact level of the information contained in non-national security systems and national security systems. For non-national security systems, SP 800-53 applies the concept of a high-water mark for categorizing the impact level of the system, as defined in FIPS 199. This means that the system is categorized according to the worst-case potential impact of a loss of confidentiality, integrity, or availability of information or an information system. For example, if loss of confidentiality was deemed to be high impact, but loss of integrity and availability were deemed to be moderate impact, the system would be considered a high-impact system. As a result, SP 800-53 contains three recommended baselines (starting points) for control selection—low, moderate, and high.

By contrast, while national security systems will use the controls in SP 800-53, the impact level will be determined using CNSSI-1253, not FIPS 199. CNSSI-1253 uses a more granular structure in which the potential impact levels of loss of confidentiality, integrity, and availability are individually used to select categorizations. As a result, while FIPS 199 has

three impact levels (low, moderate, and high), CNSSI-1253 has 27 (all possible combinations of low, moderate, and high for confidentiality, integrity, and availability).

According to an official at NIST, use of the high-water mark is easier for civilian agencies to implement for non-national security systems, and provides a more conservative approach by employing stronger controls by default. According to CNSS, retaining the more granular impact levels reduces the need for subsequent tailoring of controls. Officials involved in the harmonization effort stated that while they may attempt to reconcile the approaches in the future, there are no current plans to do so.

Security control selection. In our analysis of NIST and CNSS security control baselines for non-national security systems and national security systems, we determined that the new national security system baselines based on SP 800-53 incorporated almost all of the controls found in comparable non-national security baselines, as well as additional security controls and enhancements.[27] For example, a high-impact system under the non-national security system baseline includes 328 controls and subcontrols. The equivalent baseline for a national security system includes 397 controls and subcontrols, out of which 326 were shared between the two baselines. Both CNSS and NIST officials stated that their baselines represent the starting point for determining which controls are appropriate for an individual system and that controls and enhancements may be removed or added as needed in accordance with established guidance.

CNSS officials stated that national security systems provide unique capabilities (e.g., intelligence, cryptographic, or command and control), operate in diverse environments, and are subject to advanced cyber threats. As a result, national security systems may require more protection and thus more security controls than non-national security systems. Also, according to CNSS officials, while security controls for non-national security systems are often aimed at a broad IT environment, guidance for national security systems is developed with added specificity and a focus on vulnerabilities, threats, and countermeasures to protect classified information.

[27]A security control baseline is the set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

However, NIST officials noted some non-national security systems may require levels of protection that are equal to the levels for national security systems in order to counter cyber attacks. For example, certain high-impact non-national security systems may be supporting applications that are part of critical infrastructure. Therefore, the mission criticality of some non-national security systems may require the same control techniques used by national security systems to counter cyber attacks.

Program management controls. NIST SP 800-53, revision 3, identifies 11 program management controls that agencies are required to implement organizationwide to support all security control baselines for non-national security systems. CNSSI-1253 states that these controls are optional. A CNSS official stated that the implementation of program management controls is optional to give the CNSS community flexibility to implement them in a way that best fits their information security program organizational and operational models. DOD said it plans to address these controls in upcoming revisions to its information security guidance.

NIST and CNSS officials acknowledged that differences still exist in the harmonized guidance, and stated that the harmonization process will take time, and not all differences will be resolved during the initial harmonization effort. They stated that they have chosen to focus on issues on which they can readily achieve consensus and, if appropriate, plan to resolve remaining issues in a future revision.

Additional Supporting Guidance Is Being Developed for National Security Systems, but Detailed Time Frames for Implementation Have Not Been Established

While much of the harmonized guidance is already in use for non-national security systems, significant work remains to implement the new guidance on national security systems. For non-national security systems, OMB requires that NIST guidance be implemented within 1 year of its publication. The civilian community has been using previous versions of SP 800-53 since February 2005; thus many of the controls have already been available for use for non-national security systems.

However, while plans for implementing the harmonized information system guidance within DOD and the intelligence community have begun, full implementation may take years to complete.

Department of Defense Faces Challenges in Implementing Harmonized Guidance

While DOD officials have stated that the concepts and content in the harmonized security guidance are similar to those in existing DOD directives and instructions, the implementation process will require substantial time and effort. Officials said that transitioning to the new security controls will require in-depth planning and additional resources,

implementation will be incremental, and it will take a number of years to complete. For example, systems that are currently in development may be transitioned to the harmonized guidance, while systems that are already deployed may be transitioned only if the system undergoes a major change before its next scheduled security evaluation or review.

In order for DOD to transition to the new harmonized guidance, it plans to first revise its existing 8500 series of guidance. This process includes upcoming revisions to the information security policy documented in its directive 8500.01 and instruction 8500.2, the certification and accreditation process contained in DOD 8510.01, as well as various additional instructions and guidance. The first major step is to release the revised DOD 8500.01 and 8500.2, based on the harmonized joint task force guidance. As seen in table 2, the estimated release date for these revisions is December 2010. After this occurs, DOD plans to develop additional implementation and assessment guidance, technical instructions, and other information. The release dates for these additional items have not yet been established because their development or revision is dependent on the final publication of revisions to the 8500 series guidance.

Table 2: Estimated Dates for Revised DOD Guidance and Associated Publications

DOD publication	Estimated publication	Dependent on	Estimated publication
DODD 8500.01	December 2010	CNSSI-1253	Published
DODI 8500.2	December 2010	NIST SP 800-53	Published
		CNSSI 1253	Published
DODI 8510.01	Early 2011	NIST SP 800-37	Published
		CNSSP 6	December 2010
Other DOD implementation and assessment guides	To be determined	NIST SP 800-53A	Published

Source: GAO analysis of DOD and NIST data.

Once DOD issues guidance for implementing the joint task force's harmonized guidance, officials said that it will take several more years to incorporate the security controls into the systems' security plans. Specifically, the security plans for legacy systems will not be updated until those systems are due for recertification and reaccreditation, which could take place up to 3 years after updated DOD guidance has been released. Furthermore, DOD has not yet established milestones and performance measures for implementing the new guidance pending its issuance. Until the department develops, issues, and implements its revised policy,

including guidance on implementation time frames, potential benefits from implementing the harmonized guidance, such as reduced duplication of effort, will not be realized.

Intelligence Community Faces Challenges in Implementing Harmonized Guidance

While the intelligence community has taken steps to transition to the harmonized guidance, it faces challenges in doing so, such as developing detailed transition plans with milestones and resources for implementation.

The intelligence community has established broad transition guidance in the form of directives and standards that direct the use of CNSS policy and guidance, which in turn point to the harmonized NIST guidance.[28] The community has also developed a high-level transition plan, based on planned publication dates of harmonized guidance. In addition, guidance issued in May 2010 also states that each organization within the intelligence community shall establish its own internal transition plan and timeline based on organization-specific factors.

However, officials stated that the effort required to implement the new controls is significant in terms of the number of systems and their criticality and that implementation must be carried out in a careful, measured way. Furthermore, SP 800-53A, the publication used to assess the controls in SP 800-53, was not published until June 2010. According to CNSS and intelligence community officials, SP 800-53A needed to be issued before these agencies could complete their implementation instructions for SP 800-53 controls. Therefore, CNSS has not established policies with specific time frames for implementation of these controls.

The manager of CNSS said that the transition will be incremental, and will vary based on the complexity of the systems involved. For example, difficult-to-service embedded systems that have already been authorized, such as satellite systems, may use the current set of controls until the systems are removed from operation.

An ODNI review of intelligence community implementation plans identified several potential challenges with implementing harmonized

[28]These include Intelligence Community Directive 503, dated September 2008, which establishes intelligence community policy for IT systems security risk management and certification and accreditation, and Standard 503-2, which directs the intelligence community to use CNSSI-1253 as the authoritative source for categorizing and selecting security controls.

guidance. According to ODNI's overall transition plan issued in November 2009, a review of intelligence agency transition plans raised concerns, including the following:

- Most agencies want policies and standards to be in place before implementing the transition.
- The transition is likely to take 3 to 5 years after implementation guidance is provided.
- A phased approach is desirable and needed, but performance measures and milestones have not been defined.
- Resources, and the appropriate expertise, will need to be planned and available to implement the harmonized guidance.

The NSA official responsible for approving the operation of information systems confirmed these concerns. For example, she stated that a phased implementation approach is necessary because the agency would not be able to reaccredit and recertify all of its systems at once. Additionally, she stated that it is difficult to establish milestones and performance measures because the security of a system cannot easily be quantified. However, federal guidance and our prior work have emphasized the importance of tools such as a schedule and means to track progress to the success of IT efforts. Until supporting implementation plans with milestones, performance measures, and identified resources are developed and approved to implement the harmonized guidance, the benefits realized by the intelligence community from the harmonization effort will likely be constrained.

Key Practices May Enhance Long-Term Project Success

In prior work, we identified key practices that can help federal agencies to enhance and sustain collaboration efforts, such as the joint task force effort to harmonize information security guidance.[29] The practices include the following:

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

- *Defining and articulating a common outcome.* The compelling rationale for agencies to collaborate can be imposed externally through legislation or other directives or can come from the agencies' own perceptions of the benefits they can obtain from working together.

- *Establishing mutually reinforcing or joint strategies to achieve the outcome.* Agency strategies that work in concert with those of their partners help in aligning the partner agencies' activities, core processes, and resources to accomplish the common outcome.

- *Identifying and addressing needs by leveraging resources.* Collaborating agencies bring different levels of resources and capacities to the effort. By assessing their relative strengths and limitations, collaborating agencies can look for opportunities to address resource needs by leveraging each other's resources, thus obtaining additional benefits that would not be available if they were working separately.

- *Agreeing upon agency roles and responsibilities.* Collaborating agencies should work together to define and agree on their respective roles and responsibilities, including how the collaborative effort will be led. In doing so, agencies can clarify who will do what, organize their joint and individual efforts, and facilitate decision making.

- *Establishing compatible policies, procedures, and other means to operate across agency boundaries.* To facilitate collaboration, agencies need to address the compatibility of artifacts such as standards and policies that will be used in the collaborative effort.

- *Developing mechanisms to monitor, evaluate, and report the results of collaborative efforts.* Federal agencies engaged in collaborative efforts need to create the means to monitor and evaluate their efforts to enable them to identify areas for improvement. Reporting on these activities can help key decision makers within the agencies, as well as clients and stakeholders, to obtain feedback for improving both policy and operational effectiveness.

- *Reinforcing agency accountability for collaborative efforts through agency plans and reports.* Federal agencies can use their strategic and annual performance plans as tools to drive collaboration with other agencies and partners and establish complementary goals and strategies for achieving results. Such plans can also reinforce accountability for the collaboration by aligning agency goals and strategies with those of the collaborative efforts.

Joint task force efforts in each of these key practice areas are described in table 3.

Table 3: Joint Task Force Efforts in Key Practice Areas

Key practice	Task force activity
Defining and articulating a common outcome	The joint task force has developed a schedule that identifies the publications and time frames agreed to as an outcome of its work. Additionally, according to agency officials, NIST and CNSS have recognized the potential benefits of harmonized guidance and have collaborated through regular meetings to discuss joint work goals to support the common outcome of harmonized guidance. Task force members acknowledge that there are many areas of IT security guidance where it may be possible to collaborate, but they have not yet documented plans for future efforts. The CNSS manager stated that the committee intends to update its existing plan of action and milestones in fall 2010, but this has not yet been completed.
Establishing mutually reinforcing or joint strategies to achieve the outcome	NIST is an active participant in the annual CNSS Conference, in which discussions take place on the strategic direction for the development of policies, directives, and instructions for national security systems. One product of this conference is the plan of actions and milestones, which CNSS uses as a strategy to guide its activities. For example, the 2009 plan contained commitments to further participate in harmonization activities and to develop more CNSS guidance that supported achieving the outcome of use of the harmonized guidance.
Identifying and addressing needs by leveraging resources	Members of the joint task force, including NIST, CNSS, and NSA, work together to leverage resources and staff the groups that work on harmonizing the individual publications. However, the task force does not have an overall means of leveraging resources, such as a project plan or other document that addresses needs or identifies resources necessary to produce its publications.
Agreeing upon agency roles and responsibilities	According to task force members, there is an agreed-upon structure for the joint task force. NIST is the leader, and DOD and ODNI contribute resources as needed. However, there is no documentation of these roles and responsibilities in a charter, project plan, memorandum of understanding, or other written agreement among project participants.
Establishing compatible policies, procedures, and other means to operate across agency boundaries	CNSS has drafted a program of work and a plan of actions and milestones defining the committee's work for the upcoming year that includes harmonization of security guidance, which is the overall effort to establish compatible policies and procedures across agency boundaries. CNSS is also developing supporting guidance, such as CNSSI-1253, that directs agencies to implement the NIST publications. Furthermore, ODNI has updated its policies in support of the harmonization effort. Intelligence Community Directive 503, which is issued by ODNI, directs the use of CNSSI-1253, which, as stated above, has been harmonized with NIST guidance. The revision of existing DOD information security guidance to incorporate the harmonized guidance is still in progress.
Developing mechanisms to monitor, evaluate, and report the results of collaborative efforts	NIST publishes a schedule containing time frames for developing the task force publications that can be used to monitor the status of collaborative efforts, although two publications originally planned for release in August 2010 have been delayed until early 2011. CNSS is developing guidance, including a mechanism to monitor implementation of its instructions. The Federal CIO Council has also reported on harmonization efforts in its strategic plan. However, performance measures or mechanisms to routinely monitor, evaluate, and report on either publication development or implementation status have not been established.

Key practice	Task force activity
Reinforcing agency accountability for collaborative efforts through agency plans and reports	NIST reported on plans for and progress of efforts to harmonize IT security guidance in its Computer Security Division 2009 annual report. CNSS also reported on plans for and progress of harmonization in its April 2009 annual report. However, while CNSS policies direct it to report on the progress of implementation of its issuances, including the harmonized guidance, according to the CNSS manager, this report has not been produced.

Source: GAO analysis of joint task force member data.

To date, the task force has been successful in its efforts while having few documented or formalized processes. Task force officials stated that they believe this structure has been very effective for harmonizing information security guidance and that the success of the effort can be measured by the results achieved to date. These include the publication of three documents, planned publication of two more, and proposed future development of two additional ones. They also stated that the distinction between national security systems and non-national security systems has existed for many years, and this was the first successful effort to harmonize guidance. Officials said that key to the project's success has been strong management and technical leadership. Participants also stated that they felt the effort's informality, flexibility, and agility were strengths.

Participants acknowledged that fuller implementation of key practices, such as documenting identification of needs and leveraging of resources to address those needs, agreed-to roles and responsibilities, and monitoring and reporting on the results of its efforts, were missing; however, the officials stated that the task force has been a significant success and that more formal management practices could have been counterproductive and ineffective. For example, the task force leader stated that establishing these practices before the task force had demonstrated results would have been difficult. He stated that now that task force members have established positive relationships and become dependent on each other for technical knowledge, establishing more formal management practices may be easier.

While the task force's approach to managing the harmonization effort may not have hindered development to date, plans for future publications have slipped, in part because of the challenges of coordinating such a cross-agency effort. As the task force continues its efforts and approaches additional areas, fuller implementation of key practices, such as those that assign responsibilities and measure progress, would likely enhance its ability to sustain harmonization efforts as personnel change and resources are allocated among other agency activities.

Conclusions

Efforts to harmonize policies and guidance for national security systems and non-national security systems have made progress in producing elements of a unified information security framework. The guidance published and scheduled for publication by the joint task force constitutes a key part of the foundation of the unified framework. The task force has proposed two additional publications for consideration and acknowledged the possibility of future areas for collaboration, but plans for additional activities have yet to be finalized. The harmonization effort has the potential to reduce duplication of effort and allow more effective implementation of information security controls across interconnected systems.

To fully realize the benefits of the harmonized guidance, additional work remains to implement it. For example, supporting guidance and dates for implementation and performance measures have not been established for DOD and the intelligence community. Although, to date, the lack of documented management practices and processes has not significantly hindered the task force, as more difficult areas for harmonization are addressed, personnel change, and other agency priorities make demands upon resources, implementation of key practices for collaboration may help the task force further its progress.

Recommendations for Executive Action

To assist the joint task force in continuing its efforts to establish harmonized guidance and policies for national security systems and non-national security systems, we are making the following five recommendations. We recommend that the Secretary of Commerce direct the Director of NIST to collaborate with CNSS to

- complete plans to identify future areas for harmonization efforts, and
- consider how implementing elements of key collaborative practices, such as documenting roles and responsibilities, needs, resources, and monitoring and reporting mechanisms, may serve to sustain and enhance the harmonization effort.

We also recommend that the Secretary of Defense direct CNSS to

- collaborate with NIST to complete plans to identify future areas for harmonization efforts;

- collaborate with its member organizations, including both DOD and the intelligence community, to include milestones and performance measures in their plans to implement the harmonized CNSS policies and guidance; and

- collaborate with NIST to consider how implementing elements of key collaborative practices, such as documenting roles and responsibilities, needs, resources, and monitoring and reporting mechanisms, may serve to sustain and enhance the harmonization effort.

Agency Comments and Our Evaluation

In written comments on a draft of this report, the Secretary of Commerce concurred with our conclusions that the Departments of Commerce and Defense update plans for future collaboration, establish timelines for implementing revised guidance, and fully implement key practices for interagency collaboration in the harmonization effort. In a separate e-mail message, the NIST audit liaison clarified that Commerce also concurred with each recommendation. The department also provided technical comments, which we incorporated in the draft as appropriate. Comments from the Department of Commerce are reprinted in appendix II.

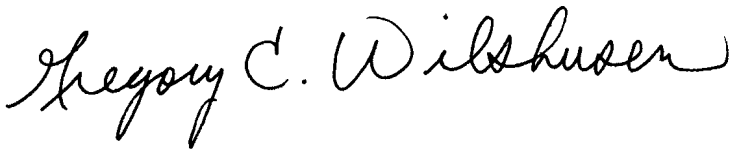
In oral comments on a draft of this report, the Senior Policy Advisor for DOD's Information Assurance and Strategy Directorate, within the Office of the Assistant Secretary of Defense (Networks and Information Integration)/DOD CIO, stated that DOD concurred with our recommendations. In addition, the CNSS manager stated in an e-mail message that the report is complete and that CNSS concurred without comment.

We also provided a draft of this report to OMB and ODNI, to which we did not make recommendations, and they both stated that they had no comments.

We are sending copies of this report to interested congressional committees, the Secretary of Commerce, and the Secretary of Defense. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

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

Sincerely,



Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objective, Scope, and Methodology

The objective of our review was to assess the progress of federal efforts to harmonize policies and guidance for national security systems and non-national security systems.

To do this, we focused on the Joint Task Force Transformation Initiative Interagency Working Group and supporting agencies within the civil, defense, and intelligence communities.[1] Specifically, we identified actions taken and planned by the Joint Task Force Transformation Initiative Interagency Working Group to harmonize information security guidance. To do this, we reviewed program plans, schedules, and performance measures related to the harmonization efforts. We also obtained and reviewed current information technology security policies, guidance, and other documentation for national security systems and non-national security systems and then conducted interviews with officials from the National Institute of Standards and Technology (NIST), Committee on National Security Systems (CNSS), Department of Defense (DOD), Office of the Director of National Intelligence (ODNI), National Security Agency (NSA), and Office of Management and Budget (OMB) to identify differences in existing guidance and plans to resolve these differences.

We also assessed efforts against criteria including prior GAO work on key practices to sustain and enhance cross-agency collaboration. We performed this assessment by reviewing documents and interviewing agency officials from NIST, CNSS, DOD, ODNI, NSA, and OMB. We identified evidence of key practices, such as documented roles and responsibilities, and mechanisms to monitor, evaluate, and report on progress, and verified our assessment with agency officials.

We conducted this performance audit from February 2010 through September 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

[1]The agencies include the National Institute of Standards and Technology, Committee on National Security Systems, U.S. Department of Defense, Office of the Director of National Intelligence, National Security Agency, and Office of Management and Budget.

Appendix II: Comments from the Department of Commerce

UNITED STATES DEPARTMENT OF COMMERCE
The Secretary of Commerce
Washington, D.C. 20230

August 27, 2010

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

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on the draft report from the U.S. Government Accountability Office (GAO) entitled "Information Security: Progress Made on Harmonizing Policies for National Security and Non-National Security Systems" (GAO-10-916).

We concur with the report's conclusions that the Department of Commerce and the Department of Defense (DoD) update plans for future collaboration, establish timelines for implementing revised guidance, and implement fully key practices for interagency collaboration in the harmonization effort. We also feel that the draft report does an outstanding job at highlighting the National Institute of Standards and Technology's (NIST) leadership in this effort. The Department of Commerce would like to offer the comments in the attached document regarding the GAO's conclusions.

We are looking forward to receiving your final report and continuing discussions with GAO regarding its conclusions. Please contact Rachel Kinney at (301) 957-8707 should you have any questions regarding this response.

Sincerely,

Gary Locke

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact name above, individuals making contributions to this report included Vijay D'Souza (assistant director), Neil Doherty, Thomas J. Johnson, Lee McCracken, David Plocher, Harold Podell, and John A. Spence.

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