DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

DHS' Efforts to Develop the Homeland Secure Data Network

Office of Information Technology

OIG-05-19

April 2005

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (Public Law 107-296) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared by the OIG as part of its DHS oversight responsibilities to promote economy, effectiveness, and efficiency within the department.

This report assesses the process used to develop and implement the Homeland Secure Data Network. It is based on interviews with DHS officials, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to the OIG, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express my appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner
Acting Inspector General

Contents

Appendices

Acronyms

C&A	Certification and Accreditation
CIO	Chief Information Officer
CONOPS	Concept of Operations
CSDN	Customs Secure Data Network
CTO	Chief Technology Officer
Customs	U.S. Customs Service (Department of the Treasury)
Deliverables	Activities and Related Documentation
DISA	Defense Information Systems Agency
DHS	Department of Homeland Security
DOD	Department of Defense
FAR	Federal Acquisition Regulations
FEDSIM	Federal Systems Integration and Management Center
FISMA	Federal Information Security Management Act
GSA	General Services Administration
HSAWG	HSDN Security Accreditation Working Group
HSDN	Homeland Secure Data Network

Contents

IPT	Integrated Product Team for HSDN
IT	Information Technology
IV&V	Independent Verification and Validation
OIG	Office of Inspector General
OMB	Office of Management and Budget
PMO	Project Management Office for HSDN
SDLC	System Development Life Cycle
SIPRNET	Secure Internet Protocol Router Network
ST&E	Security Test and Evaluation

Figures

Introduction

Terrorist attacks on U.S. interests around the world, culminating with the September 11, 2001, attack on the homeland, highlight the need for U.S. government organizations involved in terrorism prevention and response to share vital intelligence information securely in order to coordinate their activities. The *Homeland Security Act of 2002* specifically recognized this need and established procedures to address it.

Anticipating the need to share intelligence and other information securely to fulfill its homeland defense mission, the Department of Homeland Security (DHS) is streamlining and merging disparate classified networks into a single, integrated network called the Homeland Secure Data Network (HSDN). Homeland security leaders envision that HSDN will become the major secure information thoroughfare joining together intelligence agencies, law enforcement, disaster management, and front-line disaster response organizations in the common goal of protecting our nation and its citizens.

As part of its ongoing responsibilities to evaluate the effectiveness of DHS programs and activities, we conducted a review of the HSDN. The objectives of this review were to determine whether HSDN: met user needs; complied with information security standards and policies; and, was cost-effective.

We conducted fieldwork at DHS' Office of Chief Information Officer (CIO), and several DHS directorates and critical agencies. We performed our review between August and November 2004, according to generally accepted government auditing standards. See Appendix A for a description of our purpose, scope, and methodology.

Results in Brief

DHS has taken a number of key steps toward the implementation of HSDN. These include: establishing a Program Management Office (PMO) for development and implementation of HSDN; performing tasks in the planning, requirements definition, and design phases of the DHS System Development Life Cycle (SDLC) process for the new network; defining the HSDN system concept; identifying some user requirements for HSDN; and, awarding a contract for the design, development, testing, and implementation of HSDN. Further, DHS used an appropriate approach for the acquisition of HSDN.

DHS officials believed that the Department of Defense (DOD) planned to terminate DHS' access to the DOD secure network, Secret Internet Protocol Router Network[1] (SIPRNET), by December 31, 2004. Accordingly, the DHS CIO established an aggressive nine-month timeframe to implement HSDN. However, this accelerated schedule prevented DHS from adequately completing critical system development requirements. Specifically, the methods for collecting and documenting the functional and security needs of users during the requirements definition phase for the new network did not provide adequate assurance that user needs at the 600 sites will be met. Further, security implementation requirements and essential testing had not been completed one month prior to deployment. Without completing and documenting these activities in sufficient time for review and adjustment to eliminate or mitigate risk, DHS does not have assurance that HSDN complies with security standards and policies.

We are recommending that the CIO:

- Ensure that users are involved in the requirements definition process for all future implementation phases of HSDN.

- Verify that all necessary activities and documents, including certification and accreditation and thorough security control testing, are completed prior to system deployment.

[1] The Defense Information System Network has two separate internet protocol router networks: the SIPRNET and the Sensitive But Unclassified (SBU) Internet Protocol Network. The SIPRNET is an encrypted, closed loop system, meaning that it is completely separated from all other computer systems.

Background

The HSDN grew out of an initiative at the U.S. Customs Service[2] (Customs), called the Customs Secure Data Network (CSDN). The CSDN, which was estimated to cost $60 million, was intended to connect 128 sites. When Customs became part of DHS, CSDN was incorporated into the DHS consolidated information technology (IT) infrastructure. The HSDN will be comprised of secure network connections on a data communications framework that links HSDN users to data centers. These data centers will provide users with access to DHS data and will connect to other secure, federal systems through gateways.[3]

HSDN will be implemented in four phases. The first phase of the HSDN is intended to provide an integrated network for secure access to data classified as Secret.[4] In the last phase of implementation, HSDN will provide the capability of sharing Top Secret[5] information. At a cost $337 million, the HSDN will eventually connect 600 geographically dispersed DHS intelligence gathering units, operational components, and other federal, state, and local agencies involved in homeland security activities.

In the initial phase, HSDN will provide a suite of tools, including data access, secure e-mail, collaboration tools, data mining, intelligence analysis, and secure messaging[6] capabilities to 73 sites. In subsequent phases, additional HSDN capabilities will be added and extended throughout DHS and to other federal, state, and local organizations. Appendix C describes the HSDN Implementation Phases, along with the initial and future services to be provided. Appendix D provides a detailed list of the 73 sites included in Phase 1 of the HSDN implementation.

The HSDN project is organized under the overall leadership of the DHS Office of the CIO. The DHS Chief Technology Officer (CTO), who

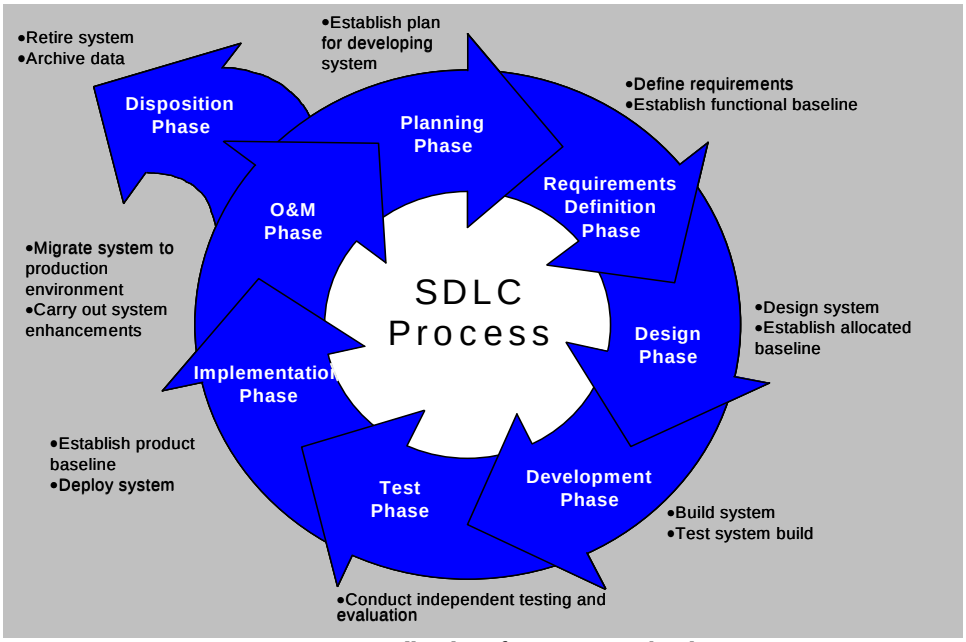
[2] The U.S. Customs Service, formally under the U.S. Department of the Treasury, divested to the U.S. Department of Homeland Security, pursuant to the *Homeland Security Act of 2002* (P.L. 107-296).
[3] A gateway is a hardware/software package that is used to interconnect networks with different protocols. The gateway has its own processor and memory, and can perform protocol and bandwidth conversions.
[4] "Secret" data is defined by Executive Order 12958 (Classified National Security Information) as information that if disclosed to unauthorized persons or compromised could cause serious damage to U.S. national security.
[5] "Top Secret" data is defined by Executive Order 12958 (Classified National Security Information) as information that if disclosed to unauthorized persons or compromised could cause exceptionally grave damage to U.S. national security.
[6] Secure e-mail allows users to encrypt e-mail messages so they cannot be read even if intercepted. Collaboration tools, such as an electronic white-board, allow people in distant offices to work together over a data communications link. Data mining provides tools to find the data you are looking for in very large databases. Intelligence analysis provides summarized intelligence data. Secure messaging handles encryption of e-mail, files, and other data sent over the network without any user intervention.

reports to the CIO, oversees the PMO, which has day-to-day responsibility for managing HSDN. The PMO has an organizational plan which describes activities employed to manage the HSDN acquisition, such as the governance structure, program office organizational structure, and staffing levels. Through a contract with the General Services Administration's (GSA) Federal Systems Integration and Management (FEDSIM) Center, the PMO built an organization for program development, implementation, and operations. On April 12, 2004, DHS awarded a contract to a prime contractor and its related partners for the design and completion of HSDN as well as integrating existing and new business processes and technologies. With its prime contractor on board, the PMO supported the near-term Phase 1 and planned for the delivery of HSDN to meet DHS classified communications objective as a part of a consolidated, secure DHS information infrastructure.

DHS is using a system development life cycle (SDLC) methodology to provide a structured approach to managing IT projects. As illustrated in Figure 1, there are eight phases in the DHS SDLC:

- *Planning Phase:* Defines the system concept from the user's perspective and establishes a comprehensive development plan.
- *Requirements Definition Phase:* Defines detailed requirements (users and technical staff) to ensure that the system will meet user requirements. Establishes a functional baseline.
- *Design Phase:* Transforms requirements into detailed design specifications. Establishes an allocated baseline, documented in the System Design Document.
- *Development Phase:* Builds the system (development team) according to the design specified during the Design Phase. Conducts development testing.
- *Test Phase:* Tests and evaluates independently to ensure that the developed system functions properly. Satisfies the requirements (including security requirements) developed in the Requirements Definition Phase and performs adequately in the host environment.
- *Implementation Phase:* Deploys system to designated production sites. Completes product baseline, including the production system, databases, an updated data dictionary, associated infrastructure, and supporting documentation.
- *Operations and Maintenance Phase:* Becomes operational. Identifies necessary system modifications. Documents them as "System Change Requests."
- *Disposition Phase:* Retires from the operational environment.

Figure 1: DHS SDLC Phases



Source: *DHS Sensitive Systems Handbook, Information Technology Security Program, DHS MD-4300, June 2003.*

DHS policy requires security to be integrated into the SDLC from the IT system's inception to the system's disposal through adequate and effective management, personnel, operational, and technical control mechanisms. In addition, OMB Circular A-130 requires that federal agencies ensure that major information systems proceed in a timely fashion toward agreed-upon milestones in an information life cycle. Also, OMB requires that information systems deliver their intended benefits, meet user requirements, and identify and offer security protections.

Findings

Challenges Remain to Ensure That HSDN User and Security Requirements Will Be Met

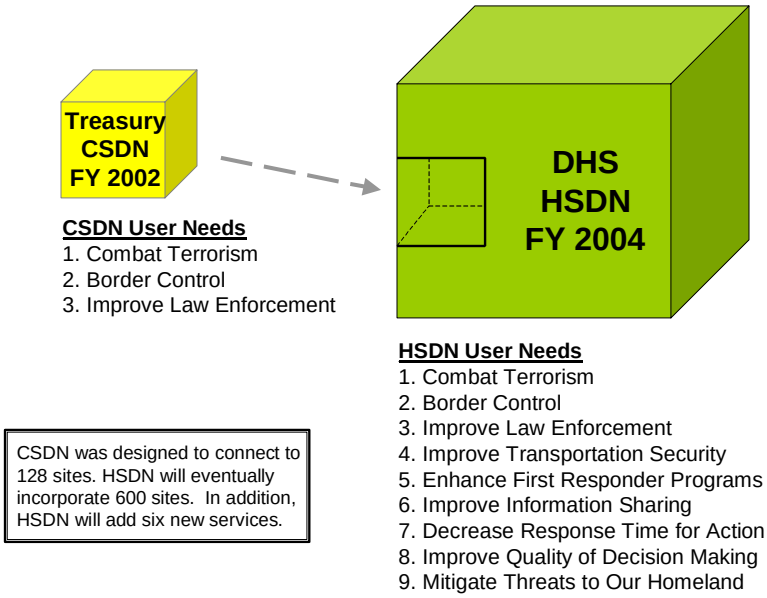
DHS has taken key steps toward the implementation of HSDN. The PMO performed tasks in the planning, requirements definition, and design phases of the DHS SDLC process for the new network. For example, DHS defined the HSDN system concept, identified some user requirements for HSDN, and awarded a contract for the design, development, testing, and implementation of HSDN. However, because DHS adopted an accelerated schedule for HSDN deployment, it did not

adequately complete key system development steps. Specifically, users were not sufficiently involved in the requirements definition phase and security implementation requirements and essential testing were not completed on schedule. As a result, DHS does not have assurance that HSDN will satisfy user needs and adequately protect classified information.

DHS Did Not Employ Sufficient Collection Methods During The HSDN Requirements Definition Phase

During the requirements definition phase for HSDN, DHS did not use sufficient methods and outreach efforts to ensure that the HSDN user community supported the functional baseline of the acquisition, and that the acquisition was based upon clearly understood needs. During 2002, prior to the creation of DHS, the former U.S. Customs defined and documented its user requirements for CSDN. When DHS acquired the CSDN program, the PMO accepted its applicability as a pilot for DHS' mission and user requirements. However, by the time the PMO presented the HSDN business case justification to the DHS Investment Review Board (November 2003), it had not validated that the requirements developed by Customs users met the needs of all DHS sites. In addition, DHS did not collect sufficient input to identify and document user requirements for the 600 HSDN sites. Figure 2 contrasts CSDN with HSDN in terms of project complexity and user requirements, as represented by lines of business.

Figure 2: Expansion of User Requirements from CSDN to HSDN



Source: OIG figure based on analysis of CSDN FY2002 and HSDN FY2004 business case justifications and capital asset plans.

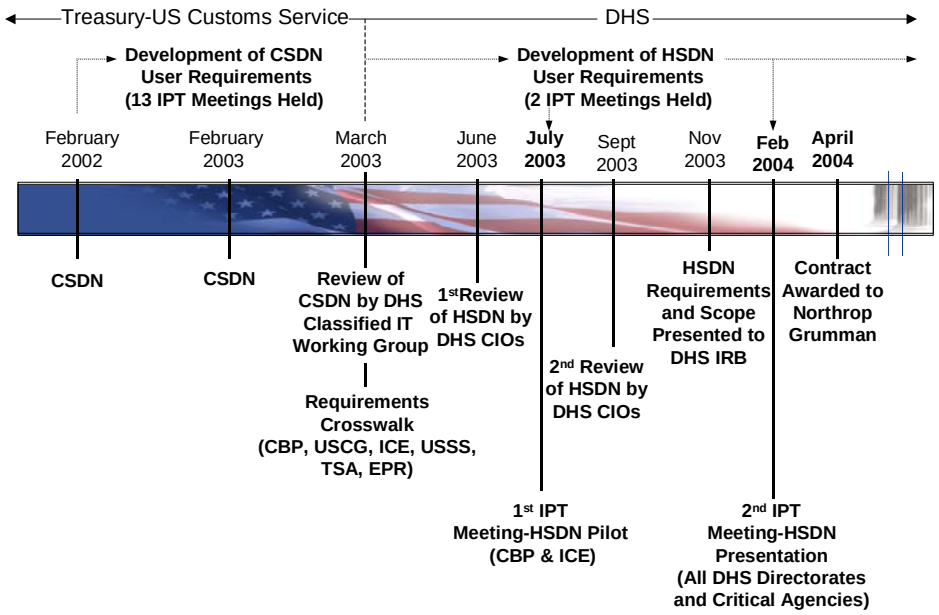
The DHS CTO said that three methods were used to identify user requirements: Integrated Product Team (IPT) meetings, HSDN Town Hall meetings, and DHS directorate and critical agency's CIO reviews. However, prior to the contract award for HSDN in April 2004, these methods did not adequately involve users in determining and documenting the functionality needed for HSDN. Figure 3 identifies all the methods employed during the requirements definition phases for CSDN and HSDN. Specifically:

- The CTO said that the IPT meetings served as an important forum for obtaining user requirements. However, as of November 2004, only two IPT meetings were held. The first meeting (July 2003) involved only two DHS components: the Bureau of Customs and Border Protection and Bureau of Immigration and Customs Enforcement.
- The second IPT meeting in February 2004, held two months before the HSDN contract was awarded, introduced current DHS users to the project, rather than identify user needs. In addition, we interviewed 18 IPT members from DHS components to determine whether user requirements had been accurately identified for the network. Five of the 18 IPT members said that they had not been involved in the

definition of user requirements. Four of the 18 IPT members said that they had not reviewed the HSDN design.

- The CTO said that Town Hall meetings were held to provide a forum for HSDN discussions and to collect user needs from user representatives. However, none of the IPT members were aware of the HSDN Town Hall meetings, and DHS did not develop minutes or attendance lists for the meetings.
- Only two meetings with DHS component CIOs were held (June 2003 and September 2003) to formally review HSDN user requirements before the contract award. However, the reviews were not detailed and the PMO did not have documentation showing that the CIOs accepted the requirements identified for the acquisition and subsequent design of HSDN.
- The PMO developed a requirements crosswalk with some DHS organizational elements in March 2003. However, other DHS components requiring secure connectivity for information sharing, IAIP, S&T, and the OIG, were not involved.

Figure 3: Requirement Definition Methods for CSDN and HSDN



Source: Adapted from HSDN Investment Review Board Presentation, November 20, 2003.

According to the DHS Sensitive Systems Handbook, users should be involved in defining the detailed requirements for new systems to ensure that the system will meet user needs. However, DHS' methods for collecting and confirming user requirements prior to contract award did not lead to assurance that user needs at the 600 sites will be met. As a result of the weaknesses in defining the user requirements for Phase 1, DHS does not have assurance that the HSDN will satisfy users' functional and security needs, and adequately protect classified information.

Key Activities - Including Security Implementation Requirements and Essential Testing - Not Completed

Many of the key activities needed to control the implementation of HSDN have not been completed. During August 2004, DHS was in the planning phase of the SDLC and intended to deploy HSDN by December 31, 2004.[7] As of November 2004, the PMO was still working on compliance with security standards and policies. In an effort to implement the HSDN within the nine-month timeframe established by the CTO, the PMO did not follow its own schedule that would allow for thorough preparation and adjustment of HSDN security, design, and development activities.

The CIO's office believed that the DOD planned to terminate DHS' access to the DOD secure network by December 31, 2004. Accordingly, the DHS CIO established an aggressive nine-month timeframe to implement HSDN and, thus, did not complete a number of key implementation steps. However, the SIPRNET Service Manager at the Defense Information Systems Agency said that there was no intent to revoke DHS access on this specific date, but to phase out services once HSDN was fully operational.

Figure 4 highlights the activities that need to be completed for HSDN. We analyzed the status of 41 HSDN key activities listed in the Task Orders. Of these deliverables, 30 of 40 (75%) missed their delivery dates. As of October 31, 2004, 28 of 41 (68%) deliverables still had not been completed. Many of these deliverables included key security planning and implementation activities to minimize the risks that the system can be compromised and to ensure that risk elimination or mitigation efforts are implemented prior to deploying the system. Essential documentation, such as the vulnerabilities assessment report, security test and evaluation report, and system certification packages, were not complete.

[7] DHS revised the HSDN implementation timeline from December 2004 to March 2005.

Figure 4: Status of Key Security, Design, and Development Activities

Aug. 23, 2004	Oct. 31, 2004	Scheduled Delivery Date	Key HSDN Security, Design, or Development Activity
NS	NS	July 28, 2004	**Security Test & Evaluation Plan**
NS	NS	May 3, 2004	**System Concept of Operations (CONOPS): Continuity of Operations Plan**
NS	NS	April 17, 2004	**Security Test** Results and Corrective actions
NS	NS	April 17, 2004	**Site/System Certification Package** (each site C&A)
NS	NS	April 17, 2004	**Vulnerabilities Assessment Report** as discovered
NS	NS	October 29, 2004	**Service Catalog**
NS	NS	November 30, 2004	**Technology Refreshment Plan** (candidate subsystems)
NS	NS	October 31, 2004	**Business Process Re-Engineering Assessment Document**
NS	NS	June 7, 2004	**HSDN Support Plan**
NS	NS	June 7, 2004	**HSDN Training Plan**
NS	NS	June 7, 2004	**Help Desk Standard Operating Procedures**
NS	NS	November 30, 2004	**Enterprise Architecture**
NS	NS	April 22, 2004	**Site Installation Plan (Prepared for each site).**
NS	NS	June 16, 2004	**Documents and Manuals**
NS	NS	July 14, 2004	**HSDN Installation Plan**
NS	NS	June 8, 2004	**Network Operation Center Standard Operating Procedures:** Disaster Recovery
NS	ID	June 8, 2004	**Security Training Plan and Curriculum**
NS	ID	June 8, 2004	**HSDN Security Plan:** Disaster Recovery Plan/Procedures
ID	ID	Date Not Established	**Privacy Impact Assessment**
ID	ID	June 8, 2004	**Contractor Facility and Physical Security Plan**
ID	ID	May 10, 2004	**Configuration Management Plan and Procedures**
ID	ID	May 3, 2004	**System CONOPS**
ID	ID	May 10, 2004	**External Interconnection Agreements**
ID	ID	April 12, 2004	**Computer Network Defense CONOPS**
ID	ID	May 10, 2004	**Computer Incident Response Team**
ID	ID	May 10, 2004	**Communication Security Plan**
ID	ID	May 3, 2004	**HSDN Master Test Plan**
ID	ID	July 28, 2004	**System Security Authorization Agreement (SSAA):** Part B
ID	C	May 17, 2004	**HSDN Quality Control Plan**
ID	C	April 12, 2004	**SSAA:** Part A
ID	C	May 3, 2004	**Government Furnished Equipment Use/Reuse Guidelines**
C	C	May 2, 2004	**HSDN Quality Assurance Surveillance Plan**
C	C	April 20, 2004	**System Architecture**
C	C	April 12, 2004	**Transition Plan**
C	C	April 12, 2004	**HSDN Deployment Plan**
C	C	April 12, 2004	**Fault Analysis Plan**
C	C	April 12, 2004	**HSDN Risk Management Plan**
C	C	April 12, 2004	**HSDN Design Document**
C	C	April 12, 2004	**Kickoff Meeting Briefing Charts**
C	C	April 12, 2004	**HSDN Project Management Plan**
C	C	April 12, 2004	**Work Breakdown Structure**

C = Completed | **ID = In Development** | **NS = Not Started** | **Security Related Activities**

Source: OIG figure based on an analysis of HSDN project deliverables.

According to DHS policy and NIST standards, security controls must be incorporated into the SDLC from the system's inception through its disposal. The PMO established the HSDN Security Accreditation Working Group (HSAWG) to involve user agencies in the Site/System Certification and testing processes. However, this group was not formed until October 2004, two months before HSDN was scheduled for deployment. During its first meeting, held on November 19, 2004, the HSAWG recognized security was a major concern and that documentation on security controls was needed.[8] As of October 31, 2004, 18 of 20 (90%) deliverables providing information for HSDN certification and accreditation were not completed. (See shaded activities in Figure 4).

The DHS Management Directive on Information Technology Systems Security[9] requires a certification and accreditation to be completed before any system can be granted authority to operate.[10] Accordingly, each of the 73 user sites must have a completed site certification and accreditation package before it can be connected to the HSDN to ensure that undetected vulnerabilities are not inherited and spread system-wide. After the packages are distributed, the sites will need time to conduct site surveys and correct any deficiencies or identify mitigating conditions prior to being connected in December 2004. As of November 19, 2004, certification packages for completion by each site before converting to the HSDN had not been distributed to the sites.[11] Accordingly, one month prior to the scheduled HSDN deployment, the site certification and accreditations were not completed.

As of November 2004, DHS had not performed essential system testing as part of the testing phase of the certification and accreditation. Specifically, the development of the security test and evaluation (ST&E) plan,[12] which was scheduled for completion in July 2004, had not yet begun. According to NIST 800-37, completing this testing and properly responding to the results should be completed during the initiation phase of the SDLC, when system requirements are established.

In addition, the HSDN Master Test Plan,[13] which was scheduled to be finished in May 2004, had not been finalized. The HSDN Master Test Plan would aid in determining whether the functional and security requirements are met,

[8] DHS Minutes of HSAWG meeting, November 19, 2004.
[9] DHS Management Directive No. 4300A, Information Technology Systems Security Management, June 2003.
[10] The primary purpose of system C&A is to promote appropriate risk management to ensure security is provided for all information collected, processed, transmitted, stored, or disseminated by systems.
[11] DHS Minutes of HSAWG meeting, November 19, 2004.
[12] The ST&E plan outlines the testing to be conducted to verify that security controls are built into HSDN function as intended and to aid in the assessment of acceptable risk.
[13] The Master Test Plan outlines the unit level, integration, operational, installation, and external interface testing that will be conducted to ensure that the system functions as intended.

facilitate assessing the effectiveness and strength of internal controls and security, and provide criteria for acceptance when passed, corrective action if failed, or eligibility for new or replaced system components. The *Federal Information Security Management Act (FISMA) of 2002*[14] requires each agency to perform testing and periodic evaluations of the effectiveness of information security and includes the testing of management, operational, and technical controls to ensure that security controls are in place to maintain risk at an acceptable level.[15]

Insofar as the Master Test Plan had not been followed, many of the IPT members who we contacted did not have the test schedule and were uncertain whether they would be involved in testing. Further, there was little or no understanding of the testing process or when and how adjustments would be made. Additionally, to improve internal controls and risk management after deployment, users may require more extensive testing than contracted, leading to additional expenditures and resource utilization that could have been avoided.

DHS Used An Appropriate Approach For The Acquisition Of HSDN

DHS employed an appropriate approach for promoting cost effectiveness of the acquisition of HSDN. To determine if the acquisition plan called for open competition, we reviewed the CSDN and HSDN OMB Exhibits 300, Task Order, and conducted interviews with the PMO. According to the information provided, the Task Order request was released under the GSA's Millennia Contract to eight top industry leaders that could serve as prime contractors for HSDN. The proposers submitted written proposals and made oral presentations to the PMO. DHS selected the Millennia contract on both technical and cost considerations as a basis for ensuring the cost effectiveness of the acquisition of services related to HSDN design, development, and implementation.

The Millennia contract is an Indefinite Delivery/Indefinite Quantity, Government-wide Acquisition Contract that fulfills the federal government's demand for large system integration and development projects by providing information technology services in a timely and cost-effective manner. The following are characteristics of the contract that support the cost effectiveness of the HSDN acquisition approach.

[14] FISMA was enacted as Title III of the E-Government Act of 2002, P.L. 107-347.
[15] Id., § 301; *codified in* 44 U.S.C. §§ 3544(a)(2)(D) and (b)(5)(A).

- The contract contains five Cost Reimbursement Task Orders, suitable for use when uncertainties in contract performance do not permit cost to be estimated with sufficient accuracy to use a fixed price contract.

- The contract is structured with award fees based on meeting development and deployment milestones, and upon achieving performance metrics as specified in Service Level Agreements.

- The contract specifies that metrics be collected and reported as factors in an Earned Value Management System. To ensure that the HSDN Project will be developed in a cost-effective manner, the Task Order implements an Earn Value Management System that complies with the ANSI/EIA Standard 748.

The PMO utilized the GSA's FEDSIM Center as the contract office representative on fee-for-service basis to provide technical and administrative support and acquisition services, including contract award and oversight. Under the Millennia contract, Northrop Grumman will perform the design, development, testing, and implementation activities for HSDN, using functional and security requirements developed by DHS.

Recommendations

To better manage the implementation of HSDN, we recommend that the CIO:

1. Ensure that users are extensively involved in the requirements definition process for all future implementation phases of HSDN.

2. Verify that all necessary activities and documents, including certification and accreditation and thorough security control testing are completed prior to system deployment.

Management Comments and Our Evaluation

We obtained written comments on a draft of this report from DHS. We have incorporated the comments where appropriate and included a copy of the comments in their entirety as Appendix B. DHS agreed with each of our recommendations. Below is a summary of DHS' response to each recommendation and our assessment of the response.

Recommendation 1: Ensure that users are extensively involved in the requirements definition process for all future implementation phases of HSDN.

The HSDN Program Director has established a senior position in the PMO as requirements lead for the program, and has assigned a PMO staff to that role to ensure that users are involved in the requirement definition process for all implementation phases of HSDN.

We accept DHS' response for ensuring that users are extensively involved in the requirements definition process for all future implementation phases of HSDN.

Recommendation 2: Verify that all necessary activities and documents, including certification and accreditation and thorough security control testing are completed prior to system deployment.

The HSDN PMO concurs that HSDN must be fully certified and accredited prior to system operation. Current certification and accreditation activities are managed by the Security group in the HSDN PMO, and occupy two senior full time PMO staff. Complying with the DHS certification and accreditation process involves development of a full documentation suite, verification of security control testing, and completion of the full process prior to system operation.

We accept DHS' response that HSDN will comply with the DHS certification and accreditation process prior to system operation.

Appendix A
Purpose, Scope, and Methodology

The objectives of our review were to determine whether HSDN: (1) met user needs; (2) complied with information security standards and policies; and, (3) was cost-effective.

We reviewed DHS efforts and requirement definition methodology - to determine whether HSDN met functional and security requirements of users - in relation to its system development life cycle methodology and applicable directives. We analyzed the Office of Management and Budget (OMB) Exhibits 300 for business case justification for CSDN and HSDN. We conducted interviews with the PMO, FEDSIM, and representatives of:

DHS Directorates or Critical Agencies

- Border and Transportation Security[16]
  - Bureau of Customs and Border Protection
  - Bureau of Immigration and Customs Enforcement
  - Transportation Security Administration
- Emergency Preparedness & Response
- Information Analysis and Infrastructure Protection
- Science & Technology
- United States Secret Service

Non-DHS Agency

- Defense Information System Agency[17]

To determine the extent to which HSDN complied with information security standards and policies, we reviewed applicable laws, federal regulations and standards, and directives. We compared security planning and implementation efforts with requirements to determine whether they were met. We reviewed the two completed certification and accreditation documents, the HSDN Risk Management Plan and the first part of the System Security Authorization Agreement. We analyzed 41 key security, design, and development activities in terms of their schedule and progress. We conducted interviews with DHS officials to assess their involvement in and concerns with security planning and testing.

To determine whether the DHS used an effective acquisition strategy for developing HSDN, we analyzed the acquisition approach and selection, OMB Exhibits 300 for CSDN and HSDN, and the DHS Task Order in relation to the Federal Acquisition Regulations (FAR) and Government Accountability Office, *Assessing Acquisition Risk for IT Investments.* In addition, we reviewed the Request for Proposals issued under the

[16] Three DHS components are from the BTS directorate.
[17] We met with Defense officials to obtain an understanding of SIPRNET requirements and DHS connectivity to SIPRNET.

Millennia contract to determine whether user requirements were translated into the contractor's Statement of Work.

We conducted our review between August and November 2004, pursuant to the Inspector General Act of 1978, as amended, and according to generally accepted government auditing standards. Major contributors to this report are listed in Appendix E.

Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

March 30, 2005

MEMORANDUM FOR: Richard Skinner, Acting Inspector General, DHS

FROM: Steve Cooper, Chief Information Officer

SUBJECT: Response by the DHS Office of the CIO to the draft report, *"Review of DHS' Efforts to Develop the Homeland Secure Data Network"*, DHS OIG Report OIG -05-XX

General Comments

Thank you for the opportunity to comment on the subject report. The results provided in the draft report comprise both observations and recommendations. The observations are valuable to our program improvement efforts and the recommendations are generally consistent with our plans.

We concur with the recommendations provided in the report and provide specific actions that we have taken related to the recommendations. We offer clarifying remarks in order to present a more current interpretation of the status of the project.

Following the field work period of the subject report, the HSDN project release plan and timeline were revised to reflect the impacts of delayed and reduced funding for the project in FY05. The revisions resulted in an abridged plan and a projected IOC date of the end of March 2005 for the classified DHS side of the network.

OIG Recommendations

The report offered two recommendations:

1. Ensure that users are involved in the requirements definition process for all future implementation phases of HSDN.

2. Verify that all necessary activities and documents, including thorough security control testing and certification and accreditation (C&A), are completed prior to system deployment.

CIO Response

The DHS Office of the CIO makes the following responses to each recommendation:

Response by the DHS Office of the CIO to the draft report, *"Review of DHS' Efforts to Develop the Homeland Secure Data Network"*

Page 2 of 2

Regarding, Recommendation #1 - "Ensure that users are involved in the requirements definition process for all future implementation phases of HSDN."

The HSDN PMO concurs that users should be involved in the requirements definition process for all implementation phases of HSDN. This has always been our plan. The HSDN Program Director has established a senior position in the PMO as requirements lead for the program and has assigned a PMO staff person to that role.

Regarding, Recommendation #2 – "Verify that all necessary activities and documents, including thorough security control testing and certification and accreditation (C&A), are completed prior to system deployment."

The HSDN PMO concurs that HSDN must be fully certified and accredited prior to system operation. This has always been our plan. Current C&A activities are managed by the Security group in the HSDN PMO, and occupy two senior full time PMO staff, and others on an as needed basis. The nature of complying with the DHS C&A process involves development of a full documentation suite, verification of security control testing, and completion of the full process prior to system operation. The system's Security Certification Package is expected to be presented for DHS certification on March 25 and shortly thereafter to DHS Accrediting Authority for system accreditation.

Additional questions regarding this response may be directed to Trisha Christian in my office at (202) 205-1403.

cc: Steve J. Pecinovsky, DHS Liaison

cc: Ryan Kociolek, USM

Appendix C
HSDN Implementation Phases and Services

Phase 1

- Secret Gateway
- Available at 73 sites:
  - DHS Headquarters
  - 6 DHS agencies: (CBP, ICE, USSS, EP&R, S&T, and TSA)
  - Three cities: (Richmond, VA; New York, NY; Albany, NY)

Phase 2

- DHS-wide deployment
- Department of Energy, Justice, and State gateways
- Temporary/remote locations brought online

Phase 3

- Governors' offices; state, local, and other U.S. domestic civilians; other federal agencies; and, emergency operation centers brought online

Phase 4

- Top Secret gateway

Initial Services

- Common software settings
- Secure e-mail
- Collaboration across people, partners, and applications
- Secure messaging
- Data mining and intelligence analysis
- End-user notification

Future Services

- Characteristics of information
- Remote access anytime, anywhere
- Advanced query
- Phone calls using computer network
- Document management
- Geospatial analysis (mapping data)
- Collection requirements management
- Secure video conferencing
- Improved productivity by tagging many objects simultaneously

Source: OIG Analysis, based on Northrop Grumman, HSDN Project Kickoff Meeting, April 2004, p.35, and DHS Investment Review Board Presentation, November 20, 2003, p.6.

Appendix D
HSDN Phase 1 Sites (June 2004)

Office	Location
BUREAU OF CUSTOMS AND BORDER PROTECTION (CBP)	
1. Office of Intelligence	Washington, DC
2. National Law Enforcement Communications Center	Orlando, FL
3. Office of Information and Technology	Newington, VA
4. National Targeting Center	Reston, VA
5. Arizona Customs Management Center (CMC)	Tucson, AZ
6. Gulf CMC	New Orleans, LA
7. Mid Pacific CMC	San Francisco, CA
8. North Atlantic CMC	Boston, MA
9. South Pacific CMC	Long Beach, CA
10. West Great Lakes CMC	Detroit, MI
11. East Texas CMC	Houston, TX
12. Mid America CMC	Chicago, IL
13. New York CMC	New York, NY
14. North Florida CMC	Tampa, FL
15. South Atlantic CMC	College Park, GA
16. South Texas CMC	Laredo, TX
17. W. Texas & NM CMC	El Paso, TX
18. East Great Lakes CMC	Buffalo, NY
19. Mid Atlantic CMC	Baltimore, MD
20. NW Great Plains CMC	Seattle, WA
21. North Pacific CMC	Portland, OR
22. South Florida CMC	Miami, FL
23. Southern California CMC	San Diego, CA
24. Port of Newark	Newark, NJ
IMMIGRATION AND CUSTOMS ENFORCEMENT (ICE)	
25. HQ	Washington DC
26. Tactical Intelligence Center	Bay St. Louis, MS
27. Air Marine Operation Center	Riverside, CA
28. Special Operations Center	Albuquerque, NM
29. Field Intelligence Unit -NE	New York, NY
30. Field Intelligence Unit- SE	Miami, FL
31. Field Intelligence Unit- SC	Houston, TX
32. Field Intelligence Unit -NC	Chicago, IL
33. Field Intelligence Unit- SW	Tucson, AZ
34. Field Intelligence Unit Pacific	Long Beach, CA
35. Special Agent in Charge	Baltimore, MD
36. Special Agent in Charge	Boston, MA
37. Special Agent in Charge	Buffalo, NY
38. Special Agent in Charge	Dallas, TX
39. Special Agent in Charge	Denver, CO
40. Special Agent in Charge	Detroit, MI
41. Special Agent in Charge	El Paso, TX
42. Special Agent in Charge	Los Angeles, CA
43. Special Agent in Charge	New Orleans, LA
44. Special Agent in Charge	New York, NY
45. Special Agent in Charge	Newark, NJ
46. Special Agent in Charge	Phoenix, AZ
47. Special Agent in Charge	San Antonio, TX
48. Special Agent in Charge	San Diego, CA
49. Special Agent in Charge	San Francisco, CA
50. Special Agent in Charge	Seattle, WA
51. Special Agent in Charge	St. Paul, MN
52. Special Agent in Charge	Tucson, AZ

Office	Location
US SECRET SERVICE (USSS)	
53. USSS	Washington, DC
54. USSS	Beltsville, MD
DHS HEADQUARTERS	
55. HQ Building	Washington, DC
56. HQ Building	Washington, DC
57. HQ Building	Washington, DC
EMERGENCY PREPAREDNESS & RESPONSE (EP&R)	
58. Headquarters	Washington, DC
59. Emergency AC	Berryville, VA
60. Region 10, MERS	Bothell, WA
61. Region 6, MERS	Denton, TX
62. Region 8, MERS	Lakewood, CO
63. Region 1, MERS	Maynard, MA
64. Region 4, MERS	Thomasville, GA
SCIENCE AND TECHNOLOGY (S&T) DIRECTORATE	
65. Northwest DC	Washington DC
66. Fort Dietrick	Frederick, MD
TRANSPORTATION SECURITY AGENCY (TSA)	
67. Colorado Springs	CO
68. Annapolis Junction	MD
69. Herndon	VA
70. Arlington	VA
STATE/LOCAL	
71. New York	NY
72. Albany	NY
73. Richmond	VA

Source: HSDN Deployment Plan, (Deliverable 21), dated June 9, 2004.

Appendix E
Major Contributors to This Report

Frank Deffer, Assistant Inspector General, Office of Information Technology

Special Projects Division
Marj Leaming, Director
Steve Harrison, Audit Manager
Louis Ochoa, Senior Auditor

Department of Homeland Security

Secretary
Deputy Secretary
General Counsel
Under Secretary, Management
DHS GAO/OIG Liaison Officer
DHS Chief Information Security Officer
DHS Office of Security
DHS Public Affairs
CIO Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Appropriate Congressional Oversight and Appropriations Committees

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528, or email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.