Department of Homeland Security
Office of Inspector General

DHS Continues to Face Challenges in the Implementation of Its OneNet Project

OIG-11-116

September 2011

Office of Inspector General

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

Homeland Security

September 28, 2011

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 as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

This report addresses the strengths and weaknesses of the DHS' management of the consolidation of its wide area network, known as OneNet. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

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

Frank Deffer
Assistant Inspector General
Information Technology Audits

Table of Contents/Abbreviations

Appendices

Abbreviations

AHRP	Application Hosting Reverse Proxy
CBP	U.S. Customs and Border Protection
CIO	Chief Information Officer
CONOPS	Concept of Operations
DHS	Department of Homeland Security
DOD	Department of Defense
EOC	Enterprise Operations Center
FEMA	Federal Emergency Management Agency
FLETC	Federal Law Enforcement Training Center
FY	fiscal year
HAG	High Assurance Gateway
HQ	headquarters
ICE	U.S. Immigration and Customs Enforcement
IPv6	Internet Protocol Version 6
ISA	interconnection security agreement
IT	information technology
ITP	Information Technology Infrastructure Transformation Program
LCCE	life cycle cost estimate
MOA	memorandum of agreement
MPLS	Multiple Protocol Label Switching
NOC	Network Operations Center
OIG	Office of Inspector General
OCIO	Office of Chief Information Officer

OMB	Office of Management and Budget
PEP	Policy Enforcement Point
ROI	return on investment
RTIC	redundant trusted Internet connection
SOC	Security Operations Center
TIC	Trusted Internet Connection
TSA	Transportation Security Administration
USCIS	United States Citizenship and Immigration Services
USCG	United States Coast Guard
USSS	United States Secret Service
VPN	virtual private network
WAN	wide area network

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

In 2005, the Department of Homeland Security began to consolidate and transform its existing individual component networks into a single world-class information technology infrastructure. To achieve this goal, the OneNet Infrastructure, an enterprise-wide integrated information technology network, was created. The goal of OneNet is to create a reliable, cost-effective information technology infrastructure platform that supports the ability to share data among components. We reviewed the Department's efforts to consolidate component networks to OneNet. Our objective was to determine the progress the Department is making in meeting its OneNet objectives.

The Department has made some progress toward consolidating the existing components' infrastructures into OneNet. Specifically, it has established a centralized Network Operations Center/Security Operations Center incident response center. Further, components are signing memorandums of agreement and converting their sites to the Multiple Protocol Label Switching architecture in accordance with OneNet requirements. Finally, the Department has established the redundant trusted Internet connection that provides a redundant network infrastructure and offers essential network services to its components.

However, the Department needs to make a number of improvements in order to implement the OneNet architecture. Specifically, it needs to establish component connections (peering) to OneNet and ensure that all components transition to the redundant trusted Internet connection. Further, it needs to complete required project management documents, and update interconnection security agreements.

We are recommending that the Department of Homeland Security Chief Information Officer complete the transition and connection (peering) of the components and develop and implement key planning documents and applicable agreements to OneNet.

Background

On July 31, 2005, the Department of Homeland Security (DHS) approved the charter for the Information Technology Infrastructure Transformation Program (ITP). The ITP represents the Department's full-scale move toward a DHS-consolidated information technology (IT) infrastructure supporting the cross-organizational missions of protecting the homeland, deterring crime, detecting and countering threats, and myriad other responsibilities. As part of the process, DHS began to consolidate its components' existing infrastructures into a single wide area network (WAN), known as OneNet.

The Department's goal for OneNet is to facilitate the ability of all DHS components to share data by integrating component networks into a single network. To achieve this goal, DHS selected U.S. Customs and Border Protection (CBP) as the network services steward to maintain and operate OneNet and its original legacy DHS Core Network. As the network steward, CBP is responsible for developing and coordinating with other components to consolidate their existing infrastructures with OneNet. Next, components converted their sites to the Multiple Protocol Label Switching (MPLS)[1] technology to provide DHS networks with enhanced redundancy, survivability, and reliability. Finally, DHS adopted a multilayered security approach by creating the Enterprise Operations Center (EOC), consisting of the Network Operations Center (NOC) and the Security Operations Center (SOC).

The concept of OneNet is to provide network segmentation between components to protect mission-critical information. To encourage an enterprise network solution throughout, DHS established Trust Zones to protect component data that cannot be shared with other components. Policy Enforcement Points (PEPs) were established to protect the security policy of the Trust Zones and allow for the sharing of services and information among the components. Figure 1 illustrates component Trust Zones and their respective connections to OneNet.

[1] MPLS is an architecture for fast packet switching and routing that provides the designation, routing, forwarding, and switching of traffic flows across a network through the use of simple, fixed-length labels.

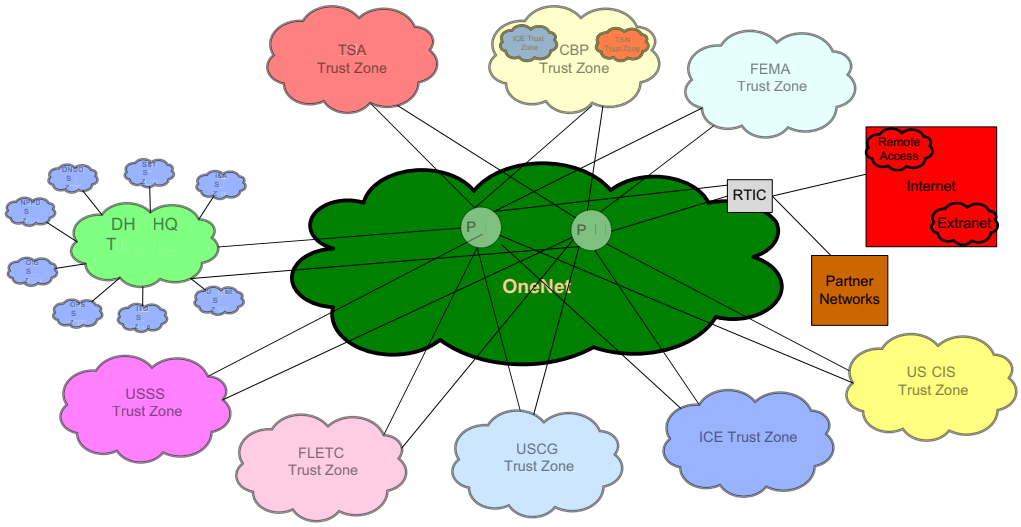

Figure 1. Trust Zone Model

DHS also implemented the Office of Management and Budget's (OMB's) Trusted Internet Connection (TIC) initiative as part of the OneNet project. The TIC initiative helps to improve the government's security posture and incident response capability by reducing and consolidating the number of external connections. To comply with the OMB TIC initiative, DHS created the DHS redundant trusted Internet connection (RTIC).[2] With the exception of the United States Coast Guard (USCG), all components must route their Internet traffic through the RTIC. USCG, as a branch of the armed forces, has been approved to use the Department of Defense (DOD) network to access the Internet. The RTIC provides four standard services:

- Outbound Internet – Public Internet access for the DHS community that is secure and policy controlled;
- Application Hosting – Infrastructure for the secure hosting of DHS resources, applications, servers and Web services to the public user community;
- Remote Access Virtual Private Network (VPN) – Secure remote access for DHS personnel to access mission-critical resources from remote locations, home, or designated disaster sites; and

[2] The DHS redundant trusted Internet connection is a certified and accredited DHS system operating in the two DHS data centers.

- Extranet Connections – Secure infrastructure for direct encrypted connection to participating government agencies and the commercial and trade community.

Figure 2 illustrates the RTIC services and connection to OneNet.

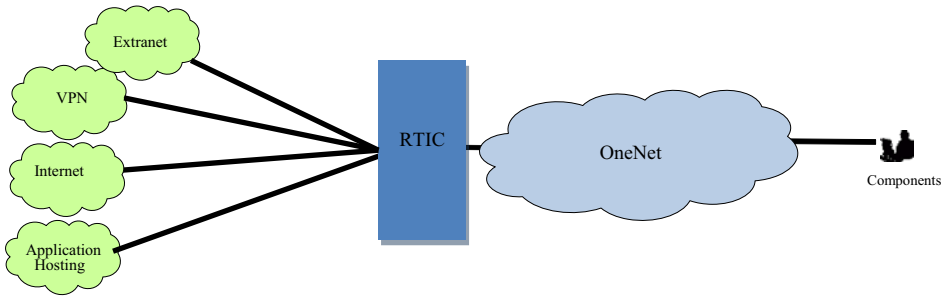

Figure 2. OneNet Diagram With RTIC Services

The OneNet life cycle cost estimate (LCCE) is $704 million per the 2011 Network Services LCCE. The project's capital investment estimates were made on the assumption that 3,759 sites will be transitioned from component legacy WANs to OneNet by fiscal year (FY) 2015. The project includes the procurement of hardware (routers and switches), software (intrusion detection), and engineering services (capacity management).

In 2005, the DHS OneNet project had a projected return on investment (ROI) of 192% over a 10-year period. In 2011, DHS revised the OneNet's projected ROI downward to 67.3% over 10 years. According to the ITP program director, a number of OMB and DHS mandates have increased the operating and maintenance, and capital investment costs of the OneNet project. Specifically, increased costs to implement the RTIC, PEPs, and Internet Protocol Version 6 (IPv6)[3] contributed to the lower ROI for the project (see figure 3).

[3] Because the current Internet protocol (Internet Protocol Version 4) has run out of addresses, agencies need to transition to IPv6. IPv6 will support a practically unlimited number of addresses worldwide.

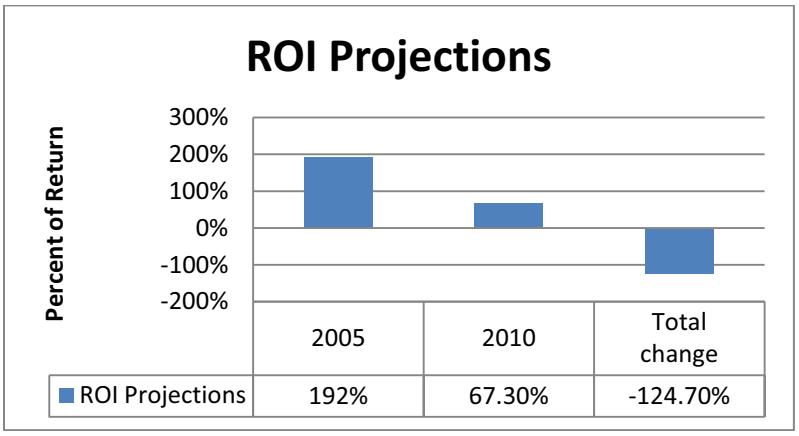

Figure 3. OneNet Return on Investment

Results of Audit

Progress Made in Implementing OneNet

DHS continues to make progress toward achieving its OneNet goals. Specifically, DHS has established a centralized NOC/SOC incident response and reporting capability in order to manage the network and resolve computer and network issues. Additionally, DHS components continue to be actively involved in supporting the transition to OneNet by signing memorandums of agreement (MOAs) and converting their sites to MPLS architecture. Finally, in June 2009, DHS established the RTIC to provide essential network services to DHS components.

Centralized NOC/SOC Services

DHS developed a NOC/SOC architecture consisting of a centralized NOC/SOC and several component-level subordinates. The central or Enterprise SOC and NOC provide management services and oversight of the DHS OneNet. Each component NOC/SOC is responsible for its individual watch areas or Trust Zones. The DHS Enterprise NOC/SOC provides guidance and coordination for component NOC/SOCs, which perform the majority of network and security incident monitoring and detection. The EOC manages the resolution of security network incidents in the corresponding domains of responsibility, network functionality, and security.

Component Progress

DHS components are also making progress in moving to the OneNet architecture. For example, all but three of the nine DHS components have signed MOAs with CBP to obtain network and security services. As the OneNet steward, CBP has elected not to prepare an MOA. MOAs are important because they identify the terms and conditions covering the services DHS will provide to components through OneNet. The MOAs include information on all OneNet core devices such as the Network Switching Nodes, policy enforcement points, RTICs and WAN devices. Table 1 provides the status of component MOAs.

Table 1. Component Status of MOA

Component	Signed MOAs	No MOAs
CBP		X
DHS HQ	X	
FEMA	X	
FLETC	X	
ICE	X	
USCIS	X	
TSA		X
USCG[4]	X	
USSS	X	

Additionally, all components have converted their sites to the MPLS architecture. The MPLS technology enables DHS and its components to read and access the audit trails captured on firewall and intrusion detection devices.

RTIC Improvements

The RTIC is a redundant network infrastructure that provides essential OneNet services (Internet, extranet, VPN, and application hosting) to support all DHS components. In FY 2009, DHS installed the second RTIC at Data Center Two in Clarksville, Virginia; the first is located in Data Center One in Stennis, Mississippi. The addition of a second trusted Internet connection creates an infrastructure that is housed at two high-availability, totally redundant and geographically diverse data centers. It was built using a flexible framework, industry best practices, DHS system engineering life cycle process, and National Institute of

[4] USCG is exempt from the OneNet migration efforts because it uses the DOD network.

Standards and Technology guidelines. The RTIC employs a layered approach that provides a high level of security, monitoring, and accountability, as depicted in figure 4.

Figure 4. Layered Approach of the RTIC

The RTIC also provides a redundant path, using multiple carrier vendors, to provide adequate security protection controls commensurate with the security requirements of the services provided.

DHS has made several improvements to the RTIC at both locations. Currently, it is planning and implementing cyber-security enhancements known as the High Assurance Gateway (HAG) and the Application Hosting Reverse Proxy (AHRP). HAG will allow the components to access information in a secure virtual environment, providing access to social media sites or otherwise prohibited contents sites that they currently cannot access. HAG also allows users (components) to browse the Internet through an enhanced firewall or a virtually hosted environment that helps to protect the user's workstation from malicious attempts to infiltrate the system. AHRP will enable components that cannot afford to move their applications to either of the two data centers to run these applications remotely from their legacy data centers. AHRP will also provide application layer access to Web and application servers.

Improvements Needed for Transition to the OneNet

DHS needs to make a number of improvements to ensure transition to OneNet. Specifically, DHS and CBP need to—

- Complete the establishment of component connections (peering) to OneNet;
- Ensure that all components transition to the RTIC;
- Complete required project management documentation; and
- Update interconnection security agreements.

Peering to OneNet Is Not Complete

All DHS components must be peered (connected) to OneNet in order for each component's transition to be complete. Sites peered to OneNet represent the number of sites associated with the OneNet domain. At present, only two components have peered all of their sites to OneNet, and the remaining seven components identified the lack of PEPs as the primary reason for their delayed transition to OneNet. PEPs support controlled cross-communication between component Trust Zones, as shown in figure 5.

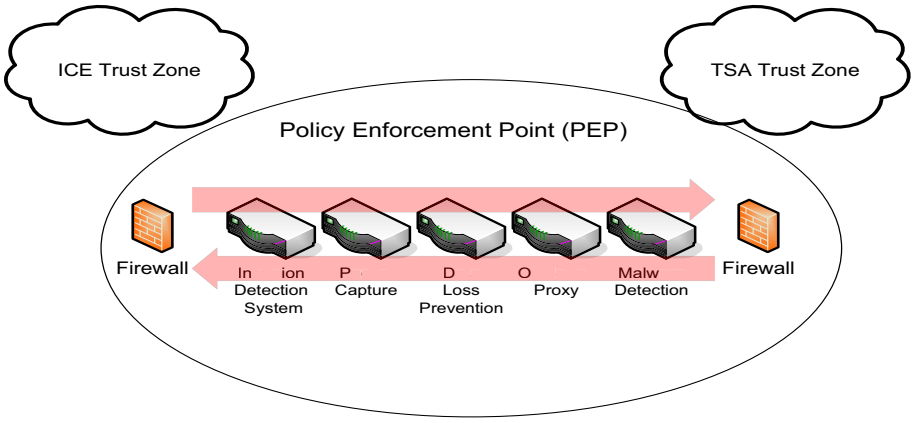

Figure 5. Components of Policy Enforcement Points

DHS components have established different and unique levels of IT security policies, along with PEPs to enforce these policies. In response, DHS' OneNet project management team revised its originally planned infrastructure to meet the components' mission driven needs and requirements. DHS Sensitive Systems Policy Management Directive 4300A and the corresponding handbook were also revised in FY 2009 to include requirements for PEPs in OneNet services. Finally, DHS' security architecture was revised to require that PEPs be implemented to separate the Trust Zones.

Transition to the RTIC Is Not Complete

Not all DHS components have completely transitioned to the RTIC. As of February 2011, two components—the Federal Law Enforcement Training Center (FLETC) and DHS headquarters—have completed transition (see table 2). Three of the remaining seven components have signed waivers with extension dates until 2012 to defer their transition to the RTIC. The Transportation Security Administration (TSA), United States Citizenship and Immigration Services (USCIS), and United States Secret Service (USSS) have not completed their respective transitions and waivers have not been granted. Waivers are required because RTIC services are mandated by OMB. USCG is exempt because it has elected to use the DOD network.

Table 2. Component Status on RTIC Transition

Components	Completed	Signed Waivers	No Waivers	Exempted
CBP		X		
DHS HQ	X			
FEMA		X		
FLETC	X			
ICE		X		
USCIS			X	
TSA			X	
USCG				X
USSS			X	

All components except USCG must route all Internet traffic through the RTICs.

DHS Has Not Developed Several Key Planning Documents for the OneNet Project

DHS has not developed several key planning documents for the overall OneNet project. Specifically, DHS has not prepared a Concept of Operations (CONOPS) for the OneNet and the RTIC projects. DHS did develop an ITP Program CONOPS that provides a brief and limited description of how DHS expects to plan and develop its network services infrastructure under OneNet. According to DHS Management Directive 102-01, Revision 01, Section 5, a CONOPS describes how DHS components would use the desired capability to fulfill its operations.

Additionally, DHS has not updated and revised its project management plan to reflect the added OMB mandates and cybersecurity enhancements. The most recent project plan for OneNet, Version 1.6 (dated March 2011), did not include an integrated project master schedule; work breakdown structure; or information on the RTICs, PEPs, and cybersecurity devices. According to the DHS interim System Engineering Life Cycle Guide, Version 2.0, Appendix B of the Acquisition Instruction/Guidebook 102-01-001, an integrated master schedule should include project resourcing, discrete work packages, internal and external dependencies, and critical paths. The development and approval of key planning documents is essential to the success of a project this size. Management should ensure that all planning documents are finalized and approved.

Interconnection Security Agreements Are Needed

DHS requires that all interconnections to DHS OneNet be documented using an interconnection security agreement (ISA). Components must complete a master ISA, which includes all transitioning systems, as part of their initial OneNet transitions. According to DHS Sensitive Systems Policy, an ISA should be—

- Described in sufficient detail to serve as a sound basis for approving a system-to-system connection;
- Signed by the authorizing official prior to operating the associated connection;
- Established in accordance with National Institute for Standards and Technology Special Publication 800-47;
- Required whenever the security policies of the interconnected systems are not identical or the systems are not administered by the same entity/authorizing official;
- Reissued every 3 years or whenever significant changes have been made to any of the interconnected systems; and
- Reviewed by component personnel as part of the annual *Federal Information Security Management Act of 2002* self-assessment.

However, OneNet ISAs are not current for all components. Specifically, three DHS components (Federal Emergency Management Agency [FEMA], DHS headquarters [HQ], and USSS) did not have OneNet ISAs, three components (TSA, FLETC, and USCG) had expired ISAs, and three components

(Immigration and Customs Enforcement [ICE], CBP, and USCIS) had current signed ISAs (see table 3).

Table 3. ISAs Received per Component

Components	Current Signed ISAs	Up for Renewal	No Documents
TSA		X	
USSS			X
USCG		X	
FEMA			X
ICE	X		
FLETC		X	
CBP	X		
HQ			X
USCIS	X		

ISAs should be prepared between DHS and each component and between each component and its trade partners.

Recommendations

We recommend that the DHS Chief Information Officer:

Recommendation #1: Complete the transition and connection (peering) of components to OneNet.

Recommendation #2: Develop, approve, and implement key planning documents, network service agreements, and interconnection security agreements.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the DHS Office of Chief Information Officer (OCIO). We have included a copy of the comments in their entirety in appendix B. Generally, the OCIO agreed with our findings and recommendations.

Recommendation #1

The OCIO concurs with Recommendation 1. The OneNet project team is working with each component to complete migrations and associated projects. This recommendation will remain open until the OCIO provides documentation to support that corrective actions are completed.

Recommendation #2

The OCIO concurs with Recommendation 2. The OneNet project team plans to update and revise its project management plan and develop a CONOPS. Additionally, the OneNet team will complete and update all MOAs and ISAs. This recommendation will remain open until the OCIO provides documentation to support that corrective actions are completed.

Appendix B
Purpose, Scope, and Methodology

The objective of our review was to determine the progress that DHS has made in consolidating components' existing infrastructure into the OneNet project. Specifically, we determined whether (1) DHS achieved its program management goals and target milestones for OneNet; (2) DHS and its components experienced any cost savings with the implementation of OneNet, and (3) DHS adequately addressed security concerns over OneNet.

We interviewed selected personnel at DHS headquarters and components facilities in the Washington, DC, area. In addition, we reviewed and evaluated DHS security policies and procedures, OneNet project plans and security architecture, the ITP charter, and other appropriate documentation.

We conducted this audit between February and June 2011 pursuant to the *Inspector General Act of 1978*, as amended, and according to 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 upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives. Major OIG contributors to the audit are identified in appendix D.

The principal OIG points of contacts for the evaluation are Frank Deffer, Assistant Inspector General, Office of Information Technology, at (202) 254-4041 and Sharon Huiswoud, Director Information Systems Audit Division, at (202) 254-5451.

Appendix B
Management Comments to the Draft Report

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

SEP 06 2011

Homeland Security

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General for IT Audits

FROM: Richard A. Spires
Chief Information Officer

SUBJECT: OIG-11-040-ITA-MGMT, *DHS Continues to Face Challenges in the Implementation of its OneNet Project*

The Department of Homeland Security (DHS) Office of the Chief Information Officer (OCIO) has reviewed the findings of the draft Office of the Inspector General (OIG) Report 11-040-ITA-MGMT, *DHS Continues to Face Challenges in the Implementation of its OneNet Project*, released July 28, 2011. OCIO's responses to OIG's draft recommendations are as follows:

Recommendation #1: Complete the transition and connection (peering) of components to OneNet.

DHS Response, August 2011: OCIO concurs.

The OneNet project management team is working with each Component to complete migrations and associated projects, such as the Policy Enforcement Points (PEPs) and Reverse Proxy, which will assist Component migrations. OCIO has targeted the second quarter of FY 2012 for completing all transition and connection of Components to OneNet.

Recommendation #2: Develop, approve, and implement key planning documents, network service agreements, and interconnection security agreements.

DHS response, August 2011: OCIO concurs.

The OneNet Project Team will update and revise its project management plan to reflect current OMB mandates and cybersecurity enhancements. The revised plan will include an integrated project master schedule that reflects project resourcing, discrete work packages, internal and external dependencies, and critical paths. The revised plan will also include information on the RTICs, PEPs, and all cybersecurity devices. OCIO has targeted the first quarter of Fiscal Year (FY) 2012 for completing the revised OneNet project management plan.

The OneNet team will also complete and update all Memoranda of Agreements (MOAs) between DHS and each Component, and all Interconnection Security Agreements (ISAs) between each Component and its trade partners. OCIO has targeted the first quarter of FY 2012 for completing and updating all MOAs and ISAs.

Additionally, the OneNet team will develop a Concept of Operations (CONOPS) for OneNet that includes the Redundant Trusted Internet Connection (RTIC) capability and that describes how Components will use the capability to fulfill their operations. OCIO has targeted the second quarter of FY 2012 for completing the CONOPS.

Appendix C
Major Contributors to this Report

Sharon Huiswoud, IT Audit Director
Sharell Matthews, IT Audit Manager
Beverly Dale, Team Leader
Anthony Nicholson, Senior IT Auditor
Robert Durst, Senior Program Analyst
Frederick Shappee, Program Analyst
Swati Nijhawan, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Chief Information Officer
Deputy Chief Information Officer
CIO Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, 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 our Hotline at 1-800-323-8603;

• Fax the complaint directly to us at (202) 254-4292;

• Email us at DHSOIGHOTLINE@dhs.gov; or

• Write to us at:
DHS Office of Inspector General/MAIL STOP 2600,
Attention: Office of Investigations - Hotline,
245 Murray Drive, SW, Building 410,
Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.