Department of Homeland Security
Office of Inspector General

Improved Management and Stronger Leadership Are Essential to Complete the OneNet Implementation (Redacted)

OIG-09-98

September 2009

Office of Inspector General

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

Homeland
Security

September 4, 2009

Preface

The Department of Homeland Security (DHS), Office of Inspector General, 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 DHS' management of its wide area network, known as OneNet. It is based on interviews with selected officials and contractor personnel, direct observations, vulnerability assessments, 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.

Richard L. Skinner

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Executive Summary 1

Background 2

Results of Audit 6

Actions Taken to Implement OneNet 6

Improved Management Oversight Needed To Complete OneNet Implementation 7

Recommendations 12

Management Comments and OIG Analysis 13

Technical Changes Can Improve OneNet Security 17

Recommendations 21

Management Comments and OIG Analysis 21

Appendices

Appendix A: Purpose, Scope, and Methodology 25

Appendix B: Management Comments to the Draft Report 26

Appendix C: Components' OneNet Implementation Status 35

Appendix D: Major Contributors to this Report 36

Appendix E: Report Distribution 37

Abbreviations

AES	Advanced Encryption Standard
CBP	Customs and Border Protection
CDP	Cisco Discovery Protocol
CIO	Chief Information Officer
CIOC	Chief Information Officer Council
CIS	Citizenship and Immigration Services
CONOPS	Concept of Operations
DCN	DHS Communication Network
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FY	Fiscal Year
HQ	Headquarters
ICCB	Interim Change Control Board
ICE	Immigration and Customs Enforcement
IP	Internet Protocol
ISS	Internet Security Systems

Table of Contents/Abbreviations

IT	Information Technology
ITP	Information Technology Infrastructure Transformation Program
MD5	Message-Digest Algorithm 5
MOA	Memorandum of Agreement
MPLS	Multiple Protocol Label Switching
NIST	National Institute of Standards and Technology
NOC/SOC	Network Operation Center/Security Operation Center
OCIO	Office of Chief Information Officer
OMB	Office of Management and Budget
PMP	Project Management Plan
PMR	Program Management Review
SIOC	Senior Infrastructure Officer Council
TACACS	Terminal Access Controller Access-Control System
TIC	Trusted Internet Connection
TSA	Transportation Security Administration
USCG	United States Coast Guard
USSS	United States Secret Service
WAN	Wide Area Network

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

The *Homeland Security Act of 2002* requires the Department of Homeland Security (DHS) to establish a secure information technology (IT) structure that enhances the communication, security, and sharing of data between components. In 2005, DHS began the process to consolidate its components' existing infrastructures into a wide area network (WAN), known as OneNet. The goal of the OneNet initiative is to help DHS consolidate its existing IT infrastructure into a more efficient and standardized architecture and to help the department improve overall cost effectiveness across the enterprise.

DHS is behind schedule in implementing OneNet, and is facing numerous challenges in achieving its network consolidation objectives. Three years have lapsed since the initial scheduled completion date of OneNet. Many OneNet implementation activities are not complete, progress to date has been limited, and cost savings have not been realized. These problems are occurring because DHS has not provided effective oversight or leadership to guide components' transition into OneNet and to ensure the completion of critical tasks for the consolidation.

Concerning security requirements, DHS has implemented adequate security controls over OneNet. We did not identify any critical vulnerabilities that could be exploited to gain unauthorized access to the network. In addition, DHS is performing adequate network and security monitoring. We determined that program officials had ensured OneNet was certified and accredited in accordance with applicable DHS information security policy. However, DHS has not configured [redacted] according to DHS security guidelines and [redacted] to provide [redacted] at its backup facility.

We are making nine recommendations to the Under Secretary for Management and Chief Information Officer. DHS concurred with five recommendations and has already begun to take actions to implement them. The resolved recommendations will remain

open until DHS provides documentation to support that the implementation of all planned corrective actions is complete. The remaining unresolved recommendations will require additional discussion between our offices before disposition. DHS' response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

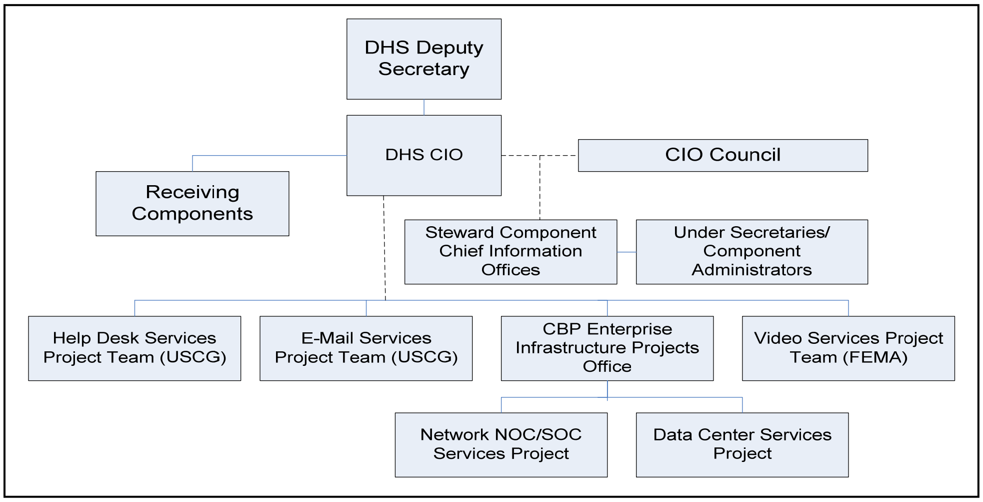
Background

On November 25, 2002, Congress enacted the *Homeland Security Act of 2002*, establishing DHS, including its mission, functions, and component organizations. As part of the Act, DHS was required to establish a secure IT infrastructure that enhances the communication, security, and sharing of data between DHS components.

In 2005, the Chief Information Officer (CIO) Council developed an operational model (see Figure 1) which assigned centralized governance and oversight responsibilities to the DHS CIO, and the decentralized execution of roles to the components that have been designated as "stewards." For example:

- Customs and Border Protection (CBP) is responsible for network services and data center services.
- United States Coast Guard (USCG) is responsible for E-mail and help desk services.
- Federal Emergency Management Agency (FEMA) is responsible for video services and serves as a backup for email and Network Operation Center/Security Operation Center (NOC/SOC) activities.

Figure 1-CIO Council Stewardship Operational Model


DHS Deputy Secretary
DHS CIO
CIO Council
Receiving Components
Steward Component Chief Information Offices
Under Secretaries/ Component Administrators
Help Desk Services Project Team (USCG)
E-Mail Services Project Team (USCG)
CBP Enterprise Infrastructure Projects Office
Video Services Project Team (FEMA)
Network NOC/SOC Services Project
Data Center Services Project

On July 31, 2005, the Deputy Secretary approved the Information Technology Infrastructure Transformation Program (ITP) Charter, which established the roles and responsibilities for the CIO, stewards, and DHS components. The focus of the ITP was to provide a single IT infrastructure that is capable of supporting the department's mission and providing unified IT services to all DHS components.[1] The ITP consists of five primary domains: data center, E-mail, help desk, network, and video services. Subsequently, a program office was established within the Enterprise Services Division of the Office of the Chief Information Officer (OCIO). Its task was to begin consolidating and modernizing the DHS IT infrastructure. In the department's October 21, 2005, response to our prior audit report, the CIO estimated that DHS would complete the consolidation of existing infrastructures into OneNet in FY 2006.[2]

In addition to the ITP Charter, the program office developed the following documents to assist DHS in managing the OneNet project:

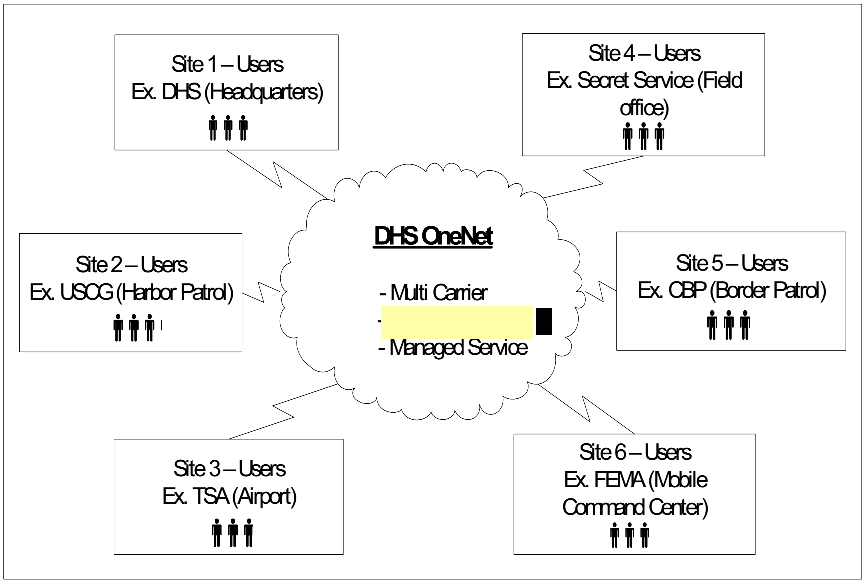
- The Project Management Plan (PMP) which contains the scope, tasks, schedule, allocated resources, and interrelationships with other projects. According to the PMP, the OneNet implementation is divided into four phases. The PMP is required to be updated at the end of each phase or when new information becomes available.
- The Program Management Review (PMR) which provides the Enterprise Services Division with a monthly snapshot of its projects, such as the ITP for OneNet.
- The DHS Security Operations Concept of Operations (CONOPS) which contains the operating procedures of the DHS SOC and the incident response procedures at component SOCs.

As the network steward, CBP is responsible for developing and coordinating with other components to consolidate their existing infrastructures into OneNet. In addition, CBP is also responsible for the overall management of the DHS NOC/SOC function. OneNet will ultimately integrate with component WANs and will provide a global communications environment that offers improved security and interoperability throughout the department. DHS envisions that OneNet will provide the components with secure data, voice, video, tactical radio, and satellite

[1] OneNet PMP, version 1.3, dated January 16, 2009.
[2] OIG-06-05, *Improved Security Required for DHS Networks* (November 2005).

communications between internal and external DHS resources. OneNet will employ [redacted] technology to provide DHS components with enhanced redundancy, survivability, and reliability.[3] Figure 2 provides a high-level view of OneNet's architecture and design.

Figure 2: OneNet Architecture and Design Overview



Before a component can migrate to OneNet, several key activities must be completed. Components must:

- Convert their sites to [redacted]
- Provide CBP with [redacted]
- Comply with the OneNet internet protocol (IP) address schemes to avoid conflicts.
- Establish and sign a memorandum of agreement (MOA) to define the roles and responsibilities between CBP and the component.

Ultimately, OneNet will help reduce the number of fragmented component networks, providing DHS with a secure in-house solution that enables centralized management and configuration capabilities. By consolidating its existing network infrastructures and data centers, DHS had estimated that it would provide a total

[redacted]

saving of $871 million. Further, DHS estimated that it would cost a total of $502 million to complete the OneNet implementation. By the end of FY 2009, DHS will have spent $149 million on OneNet implementation.

On November 20, 2007, the Office of Management and Budget (OMB) issued Memorandum 08-05 (M-08-05) announcing the Trusted Internet Connection (TIC) initiative. The purpose of the TIC initiative is to reduce the number of government external connections, including internet points of presence.

DHS is in the process of implementing OMB's TIC initiative as part of the department's OneNet project. As of April 1, 2009, one TIC was operational at [redacted] DHS expects [redacted] will become operational [redacted] by the third quarter of FY 2009. Currently, as part of OneNet, DHS' TIC provides four services to components: [redacted] DHS estimated the completion of its TIC initiative by October 30, 2009. Figure 3 depicts OneNet topology with component gateways.

Figure-3 OneNet Diagram with Components Gateways

[redacted]

Results of Audit

Actions Taken to Implement OneNet

CBP, as the network steward, has taken various steps to consolidate existing infrastructures into OneNet. The steps are designed to provide a single IT infrastructure that is capable of supporting the department's mission and providing unified IT services to all DHS components. For example, CBP has:

- Certified and accredited the [redacted] TIC in 2007 and OneNet in 2008.[4] Our review of the certification and accreditation packages revealed no significant deficiencies. As such, both OneNet and the TIC were certified and accredited in accordance with applicable DHS and OMB information security policy.
- Established a change control process to ensure that configuration changes are reviewed, authorized, and tested prior to being implemented on the routers and firewalls on OneNet.
- Established a department-wide NOC/SOC incident response and reporting capability to resolve computer and network irregularities that may affect DHS' ability to conduct its mission, on a 24 hour, 7 day a week basis.[5]
- Implemented effective controls to protect the sensitive data stored and processed by the network. We did not identify any critical vulnerabilities from our internal vulnerability assessments or external penetration testing that could be exploited to gain access to the network.

Despite these efforts, DHS faces challenges in completing its OneNet implementation. For example, DHS is experiencing delays in meeting its scheduled completion date to consolidate existing infrastructures into OneNet. In addition, components are reluctant to participate and are not subscribing to the implementation of OneNet and the TIC. More work remains to ensure that components' existing infrastructures are consolidated

[4] For certification and accreditation purposes, DHS divided the network into two systems: OneNet, and TIC.

[5] The DHS NOC is responsible for ensuring the reliable operation of OneNet and manages the configuration, operation, monitoring, and maintenance of the entire network infrastructure, supported by a network management system and a suite of network devices. The DHS SOC is responsible for monitoring the security of OneNet and manages the configuration, operation, monitoring, and maintenance of security devices deployed around the enterprise.

into OneNet and provide the department with a more efficient WAN and help DHS improve overall cost effectiveness across the enterprise.

Improved Management Oversight Needed To Complete OneNet Implementation

DHS has not provided effective oversight to ensure the timely implementation of OneNet. In addition, the department has not provided adequate leadership to guide components in their transition to OneNet and the DHS TIC. Without the required management oversight and leadership, CBP, as the OneNet steward, may not be able to fully consolidate components' existing infrastructures into OneNet. As a result, DHS may not be able to reach its ultimate goal of consolidating and modernizing its existing infrastructure and achieve projected cost savings.

<u>OneNet Implementation Is Behind Schedule</u>

As of April 2009, almost three years have lapsed since the original FY 2006 completion date. Many OneNet implementation activities are not complete and progress has been limited. The delays in implementing OneNet have stalled the department's effort. For example, in the department's FY 2007 budget, DHS had anticipated the following:[6]

- Achieving significant cost savings by shutting down redundant networks at components after the consolidation.
- Eliminating six component NOCs/SOCs after establishing the primary NOC/SOC to manage and monitor OneNet.

While the department has established the NOC/SOC to manage and monitor OneNet, ITP program officials do not anticipate that DHS will eliminate any component NOCs/SOCs. Additionally, ITP program officials and CBP personnel do not foresee that any component networks will be shut down.

In addition, DHS has not established interim milestones for the critical tasks, such as establishing the MOAs between the components and CBP and converting components' sites to [redacted] Furthermore, the PMP, which is necessary to manage the project,

[6] Department of Homeland Security Budget-in-Brief Fiscal Year 2007.

does not contain the most accurate information or reflect the current status of the network implementation.

According to an ITP program official, DHS expected components to complete their migration to OneNet by April 2010. The program official added that this new target date had been communicated orally to the components in conferences and meetings, but had not been established formally.

Status of Components' Activities

As of April 2009, six components have yet to establish MOAs with CBP.[7] Only DHS Headquarters and FEMA have MOAs with CBP. The remaining components' MOAs are in different stages of completion and review. In addition, FEMA and United States Secret Service (USSS) have yet to convert all of their sites to [redacted] Only five components (CBP, DHS Headquarters [HQ], Federal Law Enforcement Training Center [FLETC], Immigration and Customs Enforcement [ICE], and Transportation Security Administration [TSA]) have completed the conversion of their IP address schemes to OneNet to avoid conflicts. See Appendix C for a summary of components' OneNet implementation status.

Outdated Documentation

Documentation used by CBP in managing OneNet does not contain the most updated project information. The latest version of the PMP, dated January 16, 2009, had not been updated since June 21, 2006, or for more than two years. The PMP does not contain any detailed OneNet implementation activities beyond FY 2009 or include the estimated resources needed to complete the project. For example:

- Phase I-DHS Communication Network (DCN) Transformation. During this phase, the key task is to convert the DCN legacy network backbone to next-generation [redacted] service. According to the PMP, this transformation was completed in May 2005.

[7] The roles and responsibilities between CBP and components, as well as agreed upon services, are documented in MOAs.

- Phase II-OneNet Capability and Stewardship. In the PMP, key activities and milestones for this phase include: complete functional requirements analysis; develop end-state design; establish the Primary NOC and SOC capability; convert ICE to [redacted] service; and begin assuming responsibility for component edge routers. According to the PMP, this phase was completed in September 2006. However, OneNet's end-state design has not been completed because the security requirements and network functionality continue to evolve.
- Phase III-Interim Operating Capability (Component WAN Transition). According to the PMP, CBP, Citizenship and Immigration Services (CIS), ICE, DHS HQ, and TSA completed their transition to OneNet by 2007. In addition, the OneNet steward was to assume the operational control of components' core routers and the internal DCN facing firewalls.
- Phase IV-Full Operating Capability. It is noted in the ITP Charter, PMP, and CONOPS that FEMA is required to establish the alternate NOC/SOC capability. According to the PMP, this phase was to be completed by FY 2008. In addition, the PMP and CONOPS have not been updated to reflect that FEMA is no longer required to establish the alternate NOC/SOC for OneNet and that CBP has already established a backup NOC/SOC facility.

As part of the capital planning process, OMB requires agencies to institute performance measures and provide management oversight to monitor an IT project's actual performance compared to expected results. Agencies are required to prepare and update an implementation plan or PMP for IT investments. The plan should define the scope of work, identify the roles and responsibilities of key personnel, and include milestones for critical tasks. Finally, agencies are required to review and update the plan periodically to determine whether an IT investment is meeting established milestones, continues to deliver intended benefits, and is completed within budget.

Without a consolidated WAN for the department, DHS will continue to operate expensive, geographically dispersed networks and inefficiencies and service reliability issues will remain unresolved. As a result, DHS will face additional delays in achieving its projected cost savings of $841 million by consolidating its network infrastructures and data centers.

Department Leadership Needs Strengthening For Components' OneNet and TIC Migration

DHS has not provided effective leadership to ensure that components align their priorities with the department's OneNet and TIC initiatives. Components have made limited progress or shown little interest in consolidating their existing infrastructures into OneNet. Furthermore, components who are reluctant to migrate to OneNet have insisted on maintaining their own internet gateways, and are hesitant to use DHS TIC services. As a result, DHS may incur additional expenses to maintain dispersed networks and compromise network security.

As of April 2009, DHS was already behind in its TIC implementation schedule and will not meet its October 30, 2009, milestone. CIS, CBP, ICE, and TSA are not expected to complete their TIC migration until December 31, 2009. Furthermore, FEMA is not expected to complete its migration to the DHS TIC until June 2010.

None of the components were using all four services that the DHS TIC provides. Three components (FEMA, TSA, and USCG) do not use any of the four services. The majority of the other components are either using one or two services. Only DHS HQ uses three services. See Figure 4 for a list of components TIC services.

Figure 4-List of DHS TIC Services and Components' Usage

Components	DHS TIC Services			
	[redacted]	[redacted]	[redacted]	[redacted]
CBP		X		
CIS	X	X		
DHS HQ	X	X	X	
FEMA				🟥
FLETC	X			
ICE	X	X		
TSA				🟥
USCG				🟥
USSS	X			

USCG and USSS indicated that they will not complete their migration to the DHS TIC or consolidate their existing infrastructures onto OneNet. USSS decided that it would only use [redacted] service that the DHS TIC provides. In addition, USSS personnel indicated that the component was planning to submit a waiver to the DHS CIO requesting to be exempted from joining OneNet. Due to USCG's unique military background and requirements, after a February 2009 meeting between DHS and Defense Information Systems Agency (DISA) senior officials, both agencies agreed to allow USCG to be under the primary governance of DISA and transition to DISA's TIC.

With the exception of USCG, DHS has not authorized any component to maintain its own internet gateways. However, citing the specific needs to meet their mission and business requirements and security concerns, several components plan to maintain their own internet gateways or connection to the internet after their migration to the DHS TIC. Figure 5 is a list of existing component gateways.

Figure 5-List of Existing Component Gateways

Components	Number of Remaining Internet Gateways	Location
CIS	1	[redacted]
FEMA	5	[redacted]
		[redacted]
		[redacted]
		[redacted]
FLETC	2	[redacted]
		[redacted]
ICE	1	[redacted]
TSA	1	[redacted]
USCG	4	[redacted]
		[redacted]
		[redacted]
		[redacted]
USSS	1	[redacted]

ITP program officials and CBP personnel attribute part of the delays in components' OneNet consolidation and migration to the DHS TIC to the ever changing network design and increased security requirements for new DHS and OMB initiatives. In addition, due to the lack of consistency in granting security clearances and standardized suitability tests at the components, some components had concerns in relinquishing control of their network services to OneNet administrators. For example, USSS requires individuals serving as system administrators to pass a polygraph examination before being granted access to its network. However, CBP does not have the same polygraph requirement for OneNet administrators.

OMB's TIC initiative requires agencies to reduce the number of gateways to improve efficiency and security. By allowing components to maintain their own internet gateways, DHS may incur extra expenses for maintaining additional internet connections. When the TIC initiative was announced, OMB indicated that the reduction of access points to trusted internet connections would improve the situational awareness for federal agencies and allow the government to address potential threats in an expedited and efficient manner. It is also OMB's goal to minimize overall operating costs for services through economies of scale.

Due to staffing shortages, OCIO has not been able to perform its program management oversight functions to ensure that OneNet implementation is on schedule and key project documents are current. OCIO staffing shortages are indicators that DHS has not provided efficient oversight to manage OneNet implementation.

Increased risks exist that the OneNet implementation may be further delayed, preventing DHS from obtaining a consolidated IT infrastructure that is capable of supporting the department's mission and providing unified IT services to all components. Establishing interim milestones and maintaining current project documentation will provide DHS with the ability to better plan for the OneNet implementation and monitor components' progress.

Recommendations

We recommend that the Under Secretary for Management direct the CIO to:

Recommendation #1: Strengthen the department's oversight of OneNet implementation. Specifically, an agreed upon completion date and interim milestones for critical tasks to meet that date should be established to evaluate progress and determine whether critical tasks are completed timely. Components should be notified of implementation milestones.

Recommendation #2: Update the OneNet PMP and other documents periodically to reflect the current status of the implementation.

Recommendation #3: Evaluate and revise the department's current implementation strategy to ensure that components align their priorities with and participate in the department's OneNet and TIC initiatives.

Recommendation #4: Establish component implementation schedules to ensure their timely migration to OneNet and DHS TIC.

Recommendation #5: Establish a process to evaluate and address components' existing requirements regarding personnel security for the network administrators.

Management Comments and OIG Analysis

DHS response to recommendation 1

DHS did not concur with recommendation 1. Management responded that, in addition to a strong leadership team that maintains day-to-day oversight, the department has a multi-faceted structure in place to oversee and govern the OneNet program. The Interim Change Control Board (ICCB) assures that all changes are planned, engineered, tested, coordinated and approved prior to their release into the OneNet production environment; the Chief Information Security Officer monitors performance of the SOC to ensure it is compliant with DHS' security policies; the Senior Infrastructure Officer Council (SIOC) regularly reviews all current projects, schedule, cost and performance; and the Chief Information Officer Council (CIOC), develops overarching guidance and directs the effort. At the OCIO level, the DHS CIO/Deputy CIO and the CBP CIO/Deputy CIO have frequent discussions regarding the status of the OneNet implementation.

Furthermore, the department has several program level reporting mechanisms in place to review the cost, schedule and performance status, and bi-weekly updates to the SIOC regarding OneNet implementation status that is reported in a "stoplight chart." Additionally, program milestones, schedule, risks and mitigation strategies are reported to the CIO at the monthly program management reviews. To further augment these program management techniques, DHS will work with components to update and establish project plans and schedules with key milestones and specific, accurate dates pertaining to the OneNet and TIC migrations. The department will continue to monitor progress through the SIOC/CIOC and work with each component to ensure all schedules, critical tasks and milestones are being completed in a timely manner.

OIG analysis

We consider this recommendation unresolved and will require additional discussion between our offices before disposition. We maintain that DHS must strengthen its component oversight to ensure timely completion of the OneNet consolidation. Three years have lapsed since the original FY 2006 completion date. Many implementation activities are not complete and components have made limited progress or shown little interest in consolidating their existing infrastructures into OneNet. For example, none of the components are using all four services that the DHS TIC provides. The majority of components are currently using one or two services and several components plan to maintain their own internet connection after their migration to the DHS TIC.

As we noted in our report, an adequate change control process has been established to ensure that configuration changes are reviewed, authorized, and tested prior to being implemented on OneNet. However, the ICCB only has oversight on reviewing and approving proposed technical changes and does not monitor components' progress on migrating to OneNet. Furthermore, while we noted that DHS monitors the implementation through the use of a "stoplight chart" and SIOC/CIOC meetings, we maintain that the department's OneNet oversight must be strengthened. For example, management responded that the CIOC develops overarching guidance and directs the implementation effort. With the exception of the Deputy Secretary memorandum, ITP program officials were unable to provide additional documentation to support that DHS had issued any guidance to components regarding OneNet consolidation. While the security requirements and OneNet functionality continue to evolve, the PMP has not been updated to reflect any detailed implementation activities beyond FY 2009. In addition, the PMP does not include the estimated resources needed to complete the project. DHS cannot effectively measure the OneNet implementation status without an updated PMP or establishing a completion date for the consolidation and interim milestones for critical tasks such as establishing the required MOAs with CBP, migrating components' existing infrastructures into OneNet, or utilizing the services that

OneNet provides. Without strengthening components' oversight, OneNet implementation may be further delayed, preventing DHS from obtaining a consolidated IT infrastructure.

DHS response to recommendation 2

DHS concurred with recommendation 2. DHS will update the OneNet PMP, to include key milestones and dates pertaining to the OneNet transition in Fiscal Year (FY) 2010.

OIG analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved and will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS response to recommendation 3

DHS did not concur with recommendation 3. DHS noted that the department will review the OneNet and TIC implementation strategy and update as necessary with input from components. If updates or revisions of component priorities are necessary, DHS will work in concert with the SIOC/CIOC to ensure priorities are revised accordingly. While component participation must be strengthened in the future, DHS has taken a number of steps to provide effective leadership for the OneNet transition. In 2006, the Deputy Secretary issued a memorandum which not only provided clear direction to support and prioritize ITP efforts, but also directed components to plan migrations and apply both investment and Operation and Management dollars toward achieving the ITP end state in several key areas, including networks. OCIO has recommended to the Secretary's Efficiency Review Team that a Management Action Directive also be issued to reinforce the 2006 Deputy Secretary policy memorandum.

OIG analysis

While DHS noted in its response that the department did not concur with the recommendation, we conclude that the proposed corrected actions satisfy and meet the intent of this recommendation. For example, the department agreed that component participation must be strengthened in the future. DHS' proposed actions include a review of the OneNet and TIC implementation strategy. We consider this recommendation resolved and will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS response to recommendation 4

DHS concurred with recommendation 4. DHS will work with components to update and establish Project Plans and schedules with key milestones and specific, accurate dates pertaining to OneNet and TIC migrations. The department will continue to monitor progress through the SIOC/CIOC and work with each component to ensure all schedules, critical tasks and milestones are completed in a timely manner.

OIG analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved and will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS response to recommendation 5

DHS concurred with recommendation 5. The issue is being addressed by the DHS Deputy Secretary, who is leading the effort to establish suitability reciprocity within DHS, and will also be addressed by the overall Federal reform effort concerning suitability reciprocity throughout the executive branch. Suitability reciprocity is not mandated in the Federal government since no implementation order has been published. However, the DHS Office of the Chief Security Officer has taken a proactive approach along with the OCIO, and has begun negotiations with the components to come to an agreement on minimum investigative/adjudicative standards which will be acceptable to all components at DHS, and allow for reciprocity.

OIG analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved and will remain open until DHS provides documentation to support that all planned corrective actions are completed.

Technical Changes Can Improve OneNet Security

Overall, DHS has implemented effective security controls over OneNet. To assess the security posture, we interviewed selected IT personnel at OneNet's primary and backup NOC/SOC. In addition, we performed internal vulnerability assessments using [redacted] Further, we reviewed configuration settings on [redacted] for compliance with applicable DHS policy and National Institute of Standards and Technology (NIST) guidance. Finally, we performed external penetration testing using [redacted] to validate the results of our internal vulnerability assessments.[8]

<u>Security Testing Validated the Effectiveness of Controls Implemented</u>

As of January 2009, DHS had deployed more than 3,000 network devices on OneNet to include firewalls, routers, and switches. In assessing the effectiveness of system controls, we performed vulnerability assessments on 41 internal network devices, i.e., [redacted] These devices were selected based on [redacted] No critical vulnerabilities were identified that could be exploited to gain unauthorized access to OneNet. We also reviewed configuration settings [redacted] penetration testing.

To validate our internal vulnerability assessment results, we performed an external penetration test. The purpose of our external penetration test was to attempt to gain access to OneNet externally and to validate our vulnerability assessment results. First, we [redacted] We then targeted [redacted] We performed [redacted]

[8] [redacted]

[redacted] Utilizing information obtained from the discovery scans, the next step of the penetration test was to exploit any potential vulnerabilities to gain access to the network.

The results of our external penetration testing revealed that DHS has implemented effective controls to restrict access to OneNet through its external gateway, [redacted] DHS has implemented this as a protective measure to restrict access to sensitive information about the network from an outside source. The results from our configuration review and internal vulnerability assessments are consistent with this finding. [redacted] Based on our configuration review and the results of our discovery scans, the responding IP addresses are designed to communicate with other authorized routers outside the network and to facilitate traffic through the network.

The results of our penetration testing revealed that DHS has implemented effective controls to prevent unauthorized access to the network. The penetration test results support the output and analysis of the internal vulnerability testing and assessments of the security controls conducted during our audit. However, these test results are limited to [redacted] They cannot be used to support any conclusions about the security controls of OneNet through component gateways.

DHS Security Baseline Configuration Settings

While CBP has implemented effective controls on OneNet, [redacted] were not configured based on DHS security guidelines. When [redacted] are not properly configured, [redacted]

[redacted]

[redacted] We identified the following:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

DHS has developed configuration guidelines, which are a set of procedures to ensure minimum baseline security [redacted]. Components are required to ensure that DHS baseline configuration settings are implemented.

<u>NOC/SOC Disaster Recovery Capability Can Be Improved</u>

DHS has not ensured that its backup facility, located in [redacted] at its primary NOC/SOC location. [redacted]

The NOC/SOC backup facility, which became operational in January 2009, provides around the clock continuous incident analysis and monitoring of OneNet traffic. [redacted] The main function of the backup NOC/SOC is to analyze and monitor OneNet traffic. In the event of an emergency, the backup NOC/SOC is required to replicate the primary facility and provide consistent, compatible incident response and monitoring functions.

According to CBP personnel, the backup site was selected as a secondary NOC/SOC because the facility had an existing infrastructure that met DHS' requirements. In the event of an extended service disruption at the primary NOC/SOC, CBP personnel stated that [redacted]

[redacted]

[redacted] CBP personnel added that the department plans [redacted] However, no timeline has been established.

FISMA requires that each agency develop, document, and implement an agency wide information security program approved by the Director of OMB that includes, among other things, plans and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency. DHS and OMB require that contingency planning be developed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

A backup facility can provide the capabilities to replicate and restore critical applications and functions in order to resume operations in the event of a disaster. Losing computing capability and the ability to monitor, respond to, and investigate OneNet security incidents can significantly affect DHS' ability to accomplish its mission.

Recommendations

We recommend that the Under Secretary for Management direct the CIO to:

<u>Recommendation #6</u>: Implement a technical solution for OneNet to provide [redacted]

<u>Recommendation #7</u>: Strengthen [redacted] controls to restrict access and prevent unauthorized [redacted]

<u>Recommendation #8</u>: Disable [redacted] to prevent unauthorized access.

<u>Recommendation #9</u>: Establish an alternate site to supplement the backup NOC/SOC capability until the facility can be [redacted]

Management Comments and OIG Analysis

DHS response to recommendation 6

DHS concurred with recommendation 6. DHS is now taking steps to ensure that [redacted] Upon completion of the verification effort, a scan of the network will be conducted to ensure compliance. DHS expects this effort to be completed by August 31, 2009.

OIG analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved and will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS response to recommendation 7

DHS concurred with recommendation 7. DHS will change the configuration of all OneNet [redacted] to comply with the DHS MD4300A policy [redacted] will be completed by August 31, 2009. Physical security of the OneNet primary and backup NOC facilities includes strict access control and personnel security procedures, and security monitoring 24 hours a day, seven days a week. [redacted] in accordance with the DHS system security policy.

OIG analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved and will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS response to recommendation 8

DHS did not concur with recommendation 8. DHS noted that [redacted] Scans are performed regularly to discover devices running unnecessary or unauthorized services, in addition to continuous network Intrusion Detection Systems monitoring in real-time.

OIG analysis

We maintain that [redacted] were not configured based on DHS security guidelines [redacted] were not disabled. While DHS prohibits the use of [redacted] during our vulnerability assessments we identified seven instances where the service was enabled on selected [redacted] Our results revealed that [redacted] were not fully configured based on DHS configuration guidelines. DHS must strengthen its controls to ensure [redacted] are disabled on [redacted]. We consider this recommendation unresolved and will require additional discussion between our offices before disposition.

DHS response to recommendation 9

DHS did not concur with recommendation 9. DHS noted that as of December 31, 2008, the department had achieved full operating capability of the backup NOC/SOC facility. According to DHS, the backup NOC/SOC staff is sufficient to cover core critical NOC/SOC services. OneNet has fully redundant NOC/SOC server facilities with full live data replication in real-time, as well as live 24 hours a day, seven days a week NOC/SOC staff currently integrated in real time operations. Per DHS, OneNet and the backup NOC/SOC in [redacted] performed a successful Continuity of Operations failover test in January 2009 that included restoration and failover of all critical NOC/SOC applications from the backup NOC/SOC. The backup NOC/SOC can be [redacted]

OIG analysis

We maintain that due to [redacted] the secondary NOC/SOC [redacted] in the event of an extended emergency. A backup facility should provide the capabilities of replicating and restoring critical applications and functions in order to resume operations in the event of emergency. While the backup NOC/SOC is staffed to monitor the network for potential outages, [redacted]

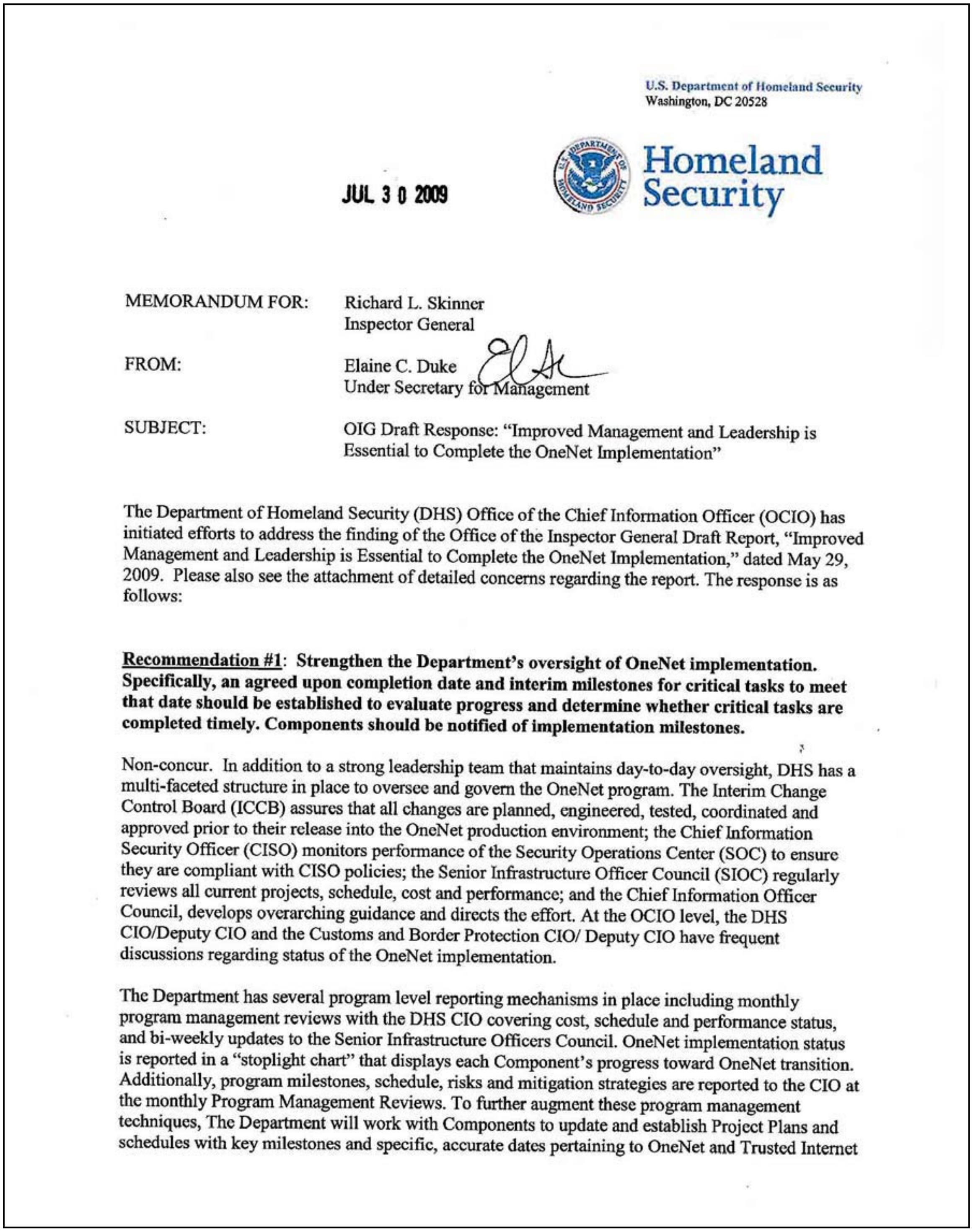
[redacted] Furthermore, due to the sensitive nature of NOC/SOC operations, these functions cannot be performed in an unprotected office environment or staffs' residences. We consider this recommendation unresolved and will require additional discussion between our offices before disposition.

The objective of our review was to determine whether DHS is implementing OneNet effectively, including related security controls, and whether projected savings and targeted milestones have been achieved. Specifically, we determined whether: (1) DHS has achieved its program management goals, including targeted milestones and projected cost savings for OneNet; (2) effective security controls have been implemented on OneNet to protect the information stored and processed by the network; (3) adequate network and security monitoring are performed for OneNet; and (4) FISMA requirements were met.

We interviewed selected personnel at DHS HQ and component facilities in the Washington, D.C. area; primary NOC/SOC personnel in [redacted]; and backup NOC/SOC personnel in [redacted]. In addition, we reviewed and evaluated DHS' security policies and procedures, OneNet project plans and technical descriptions, the ITP charter, and other appropriate documentation. During the audit, we used software tools, [redacted], to detect, analyze, and evaluate the effectiveness of the security controls implemented on selected OneNet [redacted] We also performed external penetration testing using [redacted] to validate the results of our internal vulnerability assessments. Upon completion of the assessments, we provided program officials with the technical reports detailing the specific vulnerabilities detected on OneNet network devices and the actions needed for remediation.

We conducted this audit between January and April 2009 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Major OIG contributors to the audit are identified in Appendix D.

The principal OIG points of contact for the evaluation are Frank Deffer, Assistant Inspector General, Office of Information Technology, at (202) 254-4041 and Edward G. Coleman, Director, Information Security Audit Division, at (202) 254-5444.



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

Homeland Security

JUL 3 0 2009

MEMORANDUM FOR: Richard L. Skinner
Inspector General

FROM: Elaine C. Duke
Under Secretary for Management

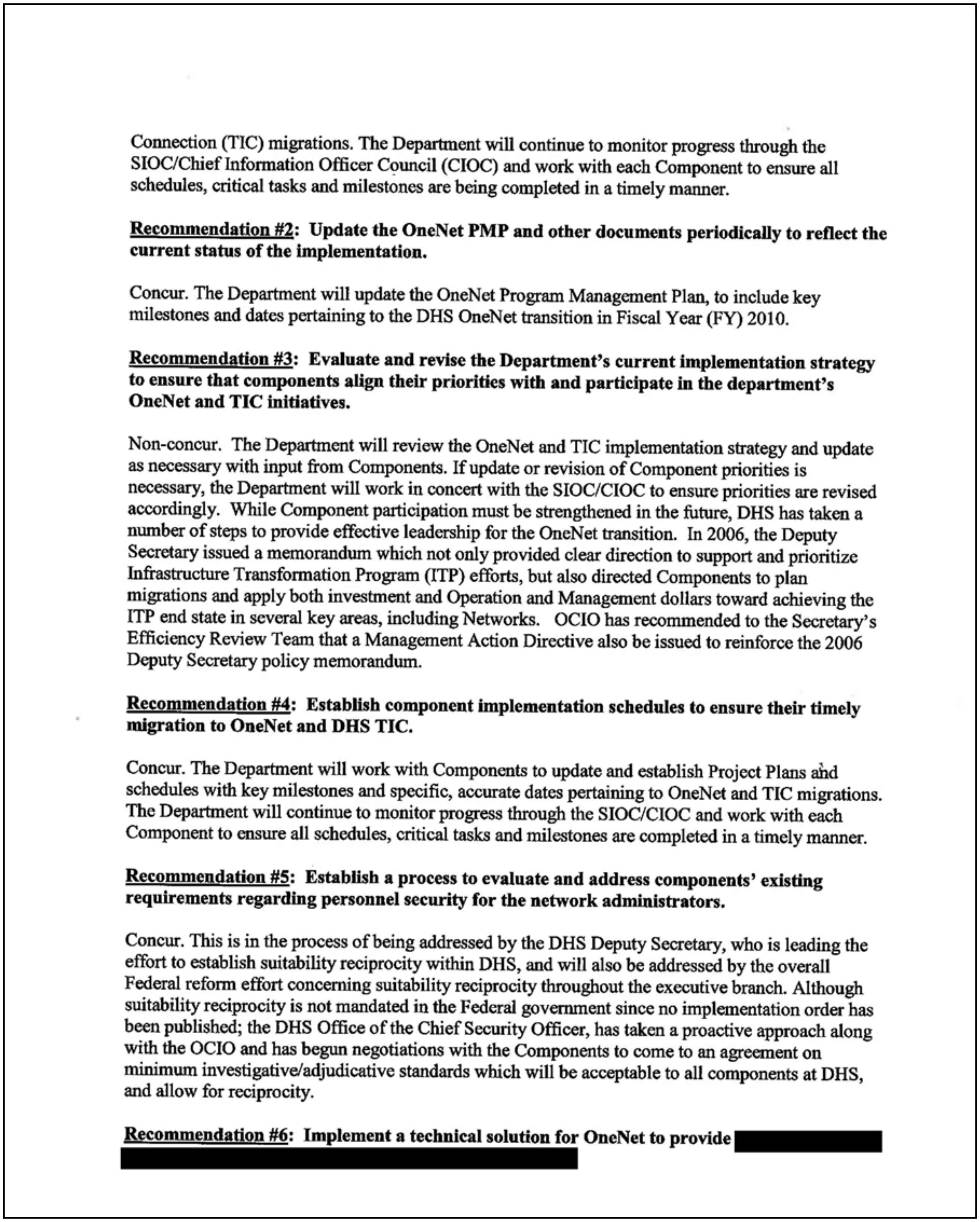
SUBJECT: OIG Draft Response: "Improved Management and Leadership is Essential to Complete the OneNet Implementation"

The Department of Homeland Security (DHS) Office of the Chief Information Officer (OCIO) has initiated efforts to address the finding of the Office of the Inspector General Draft Report, "Improved Management and Leadership is Essential to Complete the OneNet Implementation," dated May 29, 2009. Please also see the attachment of detailed concerns regarding the report. The response is as follows:

Recommendation #1: **Strengthen the Department's oversight of OneNet implementation. Specifically, an agreed upon completion date and interim milestones for critical tasks to meet that date should be established to evaluate progress and determine whether critical tasks are completed timely. Components should be notified of implementation milestones.**

Non-concur. In addition to a strong leadership team that maintains day-to-day oversight, DHS has a multi-faceted structure in place to oversee and govern the OneNet program. The Interim Change Control Board (ICCB) assures that all changes are planned, engineered, tested, coordinated and approved prior to their release into the OneNet production environment; the Chief Information Security Officer (CISO) monitors performance of the Security Operations Center (SOC) to ensure they are compliant with CISO policies; the Senior Infrastructure Officer Council (SIOC) regularly reviews all current projects, schedule, cost and performance; and the Chief Information Officer Council, develops overarching guidance and directs the effort. At the OCIO level, the DHS CIO/Deputy CIO and the Customs and Border Protection CIO/ Deputy CIO have frequent discussions regarding status of the OneNet implementation.

The Department has several program level reporting mechanisms in place including monthly program management reviews with the DHS CIO covering cost, schedule and performance status, and bi-weekly updates to the Senior Infrastructure Officers Council. OneNet implementation status is reported in a "stoplight chart" that displays each Component's progress toward OneNet transition. Additionally, program milestones, schedule, risks and mitigation strategies are reported to the CIO at the monthly Program Management Reviews. To further augment these program management techniques, The Department will work with Components to update and establish Project Plans and schedules with key milestones and specific, accurate dates pertaining to OneNet and Trusted Internet



Connection (TIC) migrations. The Department will continue to monitor progress through the SIOC/Chief Information Officer Council (CIOC) and work with each Component to ensure all schedules, critical tasks and milestones are being completed in a timely manner.

<u>Recommendation #2</u>: Update the OneNet PMP and other documents periodically to reflect the current status of the implementation.

Concur. The Department will update the OneNet Program Management Plan, to include key milestones and dates pertaining to the DHS OneNet transition in Fiscal Year (FY) 2010.

<u>Recommendation #3</u>: Evaluate and revise the Department's current implementation strategy to ensure that components align their priorities with and participate in the department's OneNet and TIC initiatives.

Non-concur. The Department will review the OneNet and TIC implementation strategy and update as necessary with input from Components. If update or revision of Component priorities is necessary, the Department will work in concert with the SIOC/CIOC to ensure priorities are revised accordingly. While Component participation must be strengthened in the future, DHS has taken a number of steps to provide effective leadership for the OneNet transition. In 2006, the Deputy Secretary issued a memorandum which not only provided clear direction to support and prioritize Infrastructure Transformation Program (ITP) efforts, but also directed Components to plan migrations and apply both investment and Operation and Management dollars toward achieving the ITP end state in several key areas, including Networks. OCIO has recommended to the Secretary's Efficiency Review Team that a Management Action Directive also be issued to reinforce the 2006 Deputy Secretary policy memorandum.

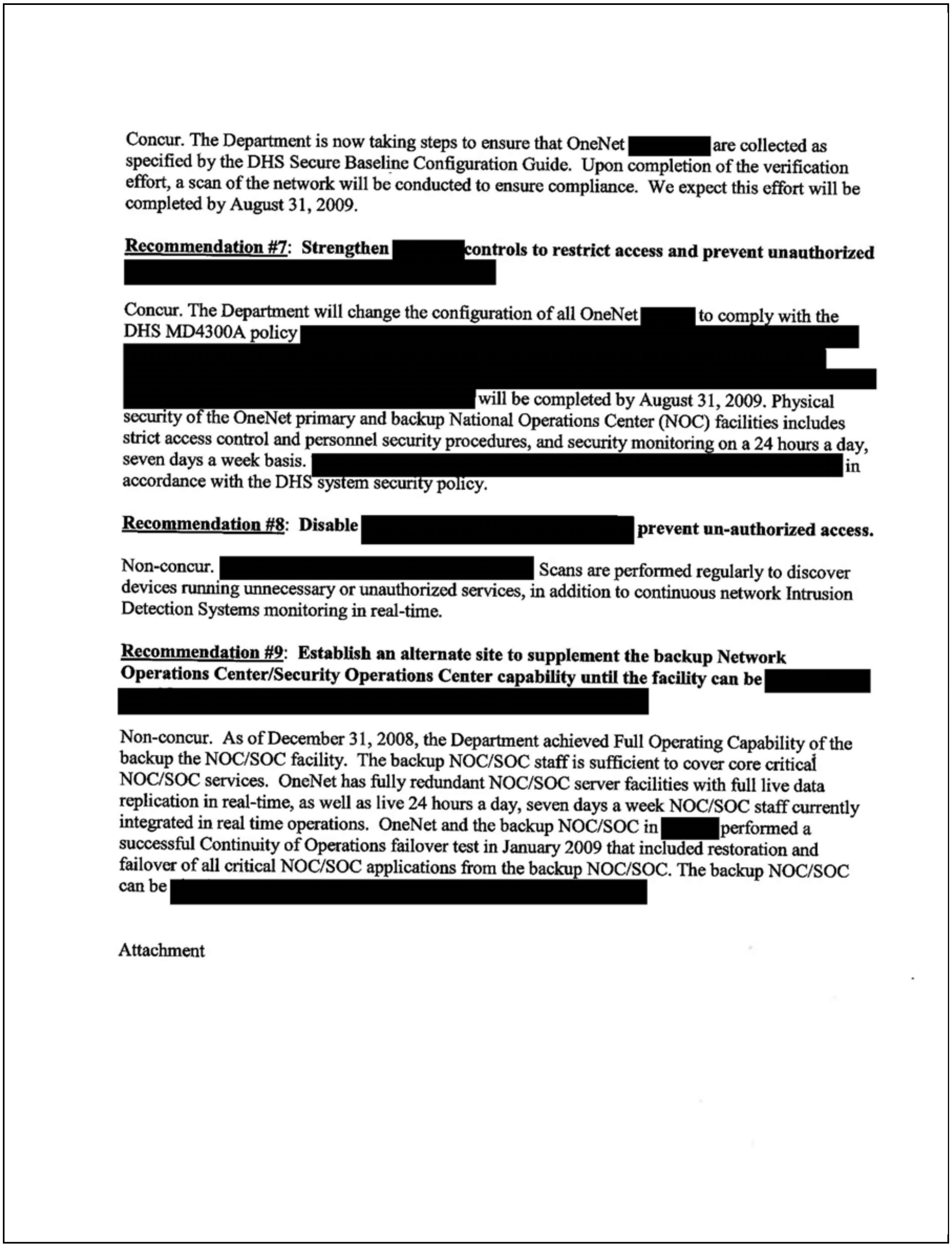
<u>Recommendation #4</u>: Establish component implementation schedules to ensure their timely migration to OneNet and DHS TIC.

Concur. The Department will work with Components to update and establish Project Plans and schedules with key milestones and specific, accurate dates pertaining to OneNet and TIC migrations. The Department will continue to monitor progress through the SIOC/CIOC and work with each Component to ensure all schedules, critical tasks and milestones are completed in a timely manner.

<u>Recommendation #5</u>: Establish a process to evaluate and address components' existing requirements regarding personnel security for the network administrators.

Concur. This is in the process of being addressed by the DHS Deputy Secretary, who is leading the effort to establish suitability reciprocity within DHS, and will also be addressed by the overall Federal reform effort concerning suitability reciprocity throughout the executive branch. Although suitability reciprocity is not mandated in the Federal government since no implementation order has been published; the DHS Office of the Chief Security Officer, has taken a proactive approach along with the OCIO and has begun negotiations with the Components to come to an agreement on minimum investigative/adjudicative standards which will be acceptable to all components at DHS, and allow for reciprocity.

<u>Recommendation #6</u>: Implement a technical solution for OneNet to provide [redacted]



Concur. The Department is now taking steps to ensure that OneNet [redacted] are collected as specified by the DHS Secure Baseline Configuration Guide. Upon completion of the verification effort, a scan of the network will be conducted to ensure compliance. We expect this effort will be completed by August 31, 2009.

<u>Recommendation #7</u>: Strengthen [redacted] controls to restrict access and prevent unauthorized [redacted]

Concur. The Department will change the configuration of all OneNet [redacted] to comply with the DHS MD4300A policy [redacted] will be completed by August 31, 2009. Physical security of the OneNet primary and backup National Operations Center (NOC) facilities includes strict access control and personnel security procedures, and security monitoring on a 24 hours a day, seven days a week basis. [redacted] in accordance with the DHS system security policy.

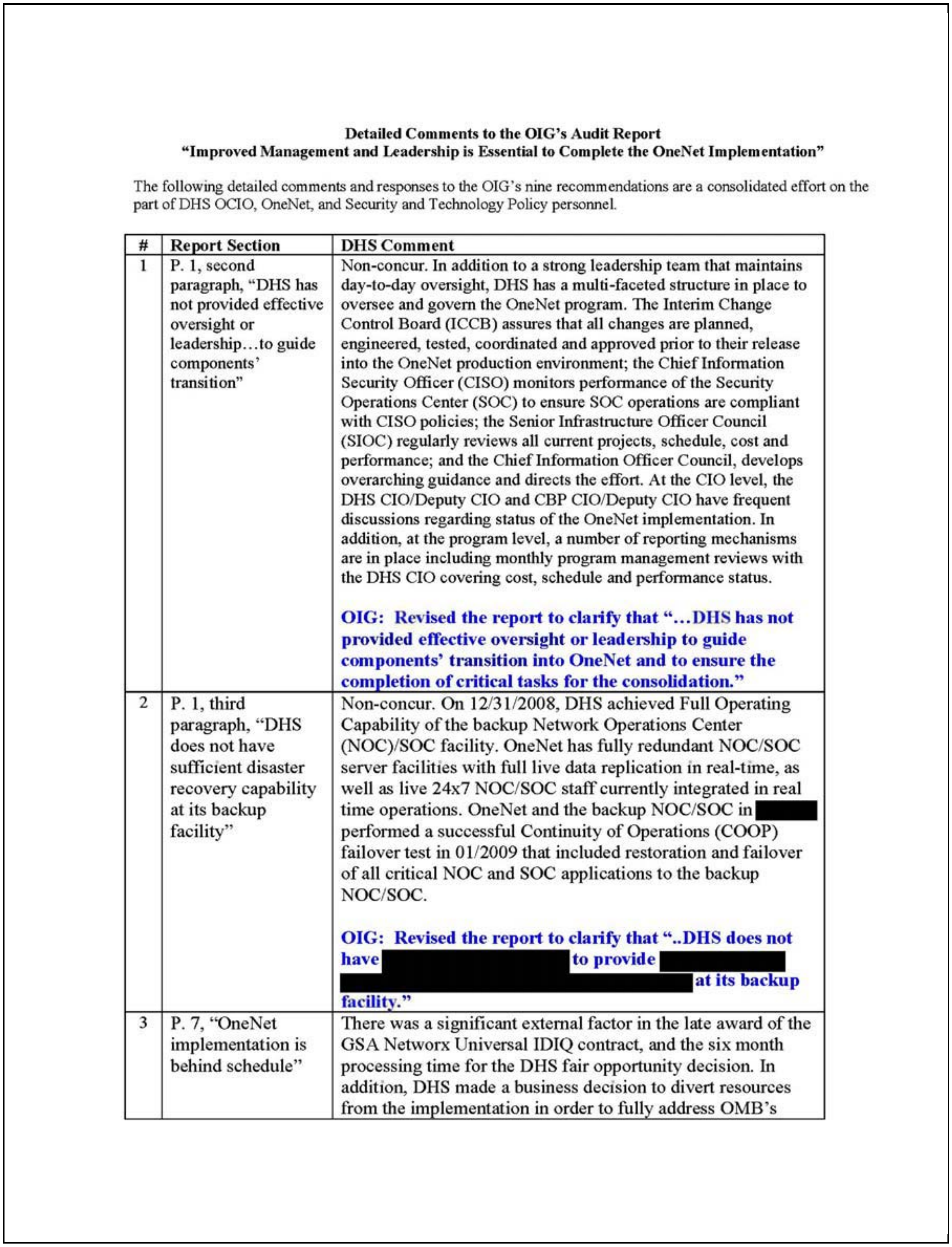
<u>Recommendation #8</u>: Disable [redacted] prevent un-authorized access.

Non-concur. [redacted] Scans are performed regularly to discover devices running unnecessary or unauthorized services, in addition to continuous network Intrusion Detection Systems monitoring in real-time.

<u>Recommendation #9</u>: Establish an alternate site to supplement the backup Network Operations Center/Security Operations Center capability until the facility can be [redacted]

Non-concur. As of December 31, 2008, the Department achieved Full Operating Capability of the backup the NOC/SOC facility. The backup NOC/SOC staff is sufficient to cover core critical NOC/SOC services. OneNet has fully redundant NOC/SOC server facilities with full live data replication in real-time, as well as live 24 hours a day, seven days a week NOC/SOC staff currently integrated in real time operations. OneNet and the backup NOC/SOC in [redacted] performed a successful Continuity of Operations failover test in January 2009 that included restoration and failover of all critical NOC/SOC applications from the backup NOC/SOC. The backup NOC/SOC can be [redacted]

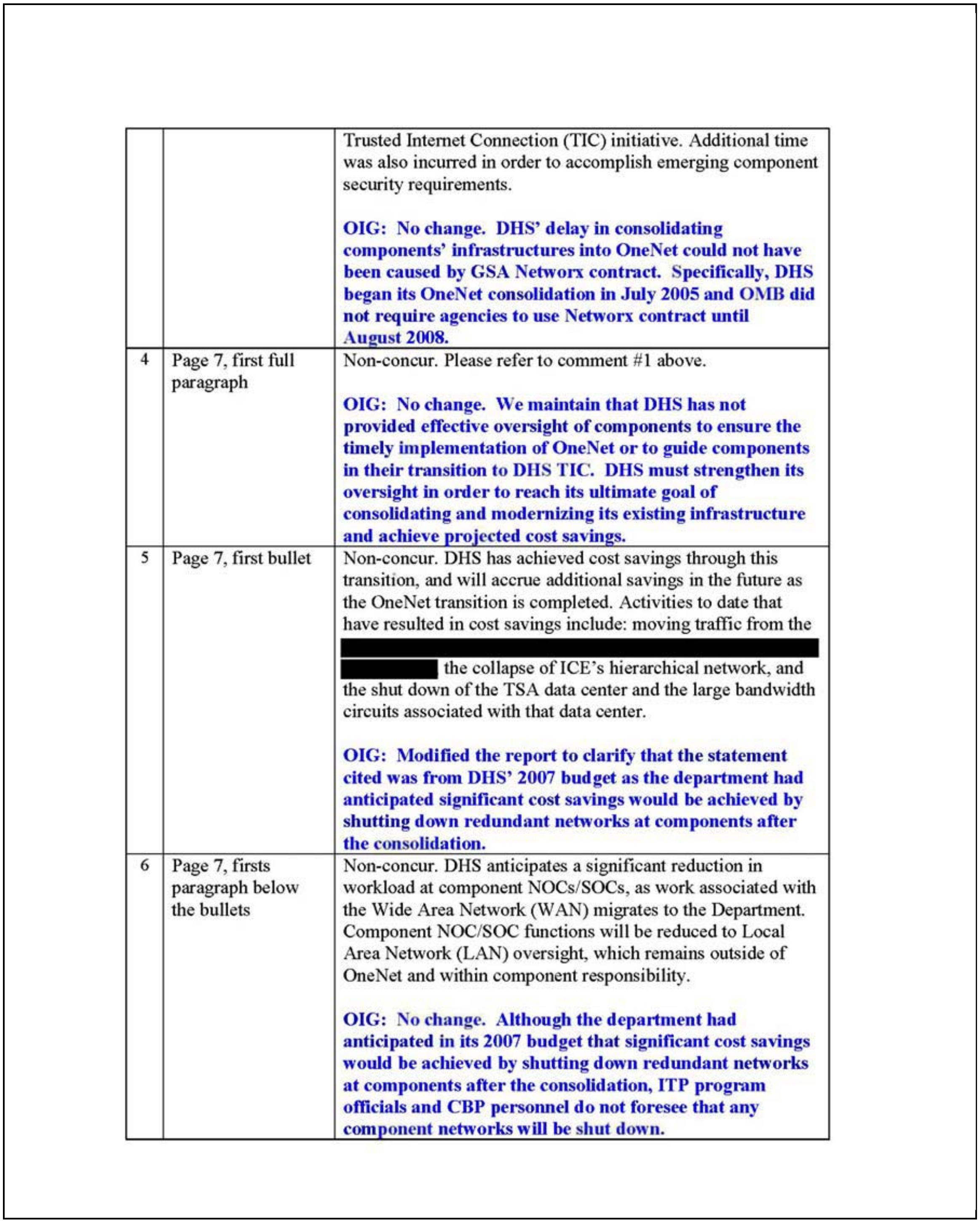
Attachment



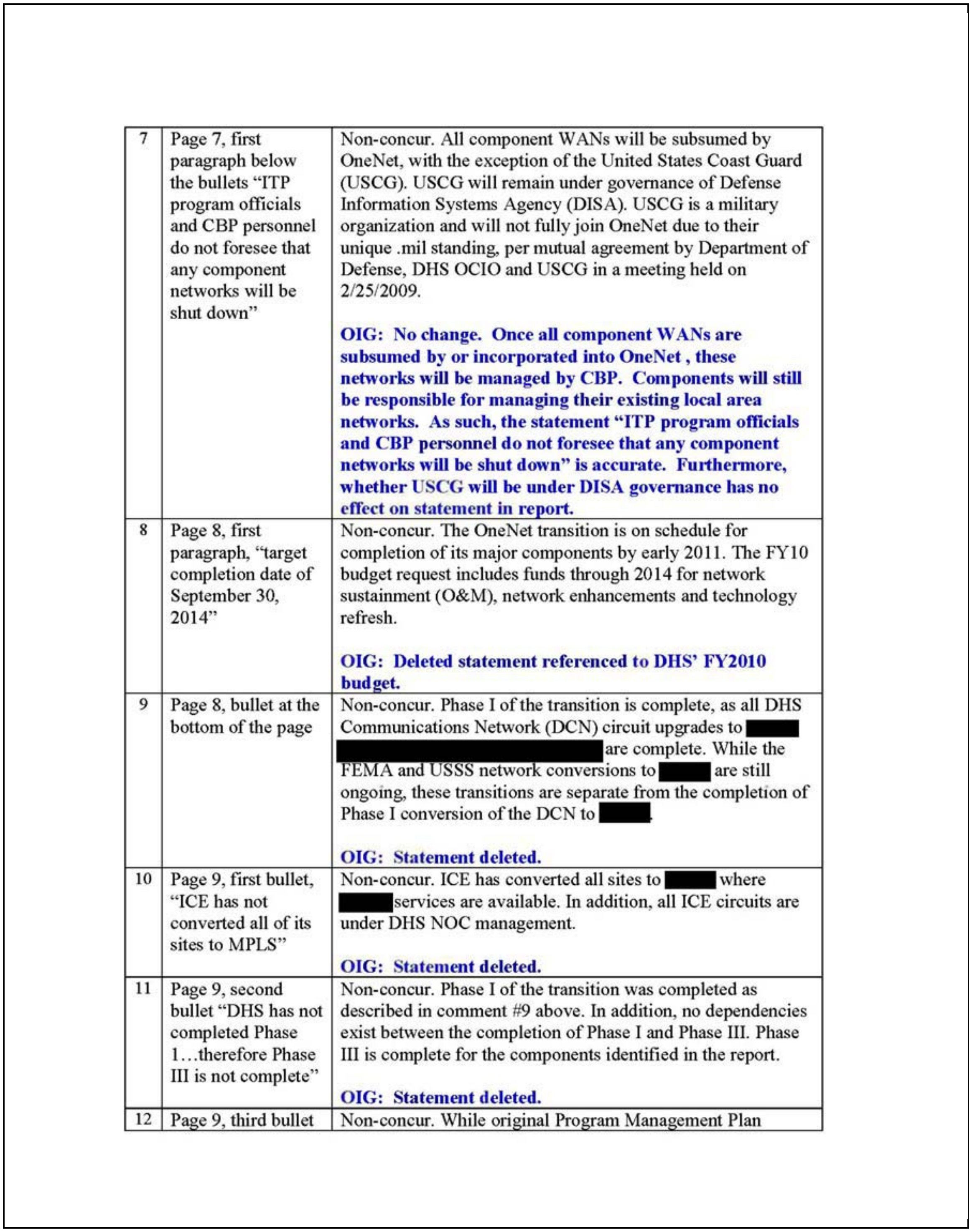
Detailed Comments to the OIG's Audit Report
"Improved Management and Leadership is Essential to Complete the OneNet Implementation"

The following detailed comments and responses to the OIG's nine recommendations are a consolidated effort on the part of DHS OCIO, OneNet, and Security and Technology Policy personnel.

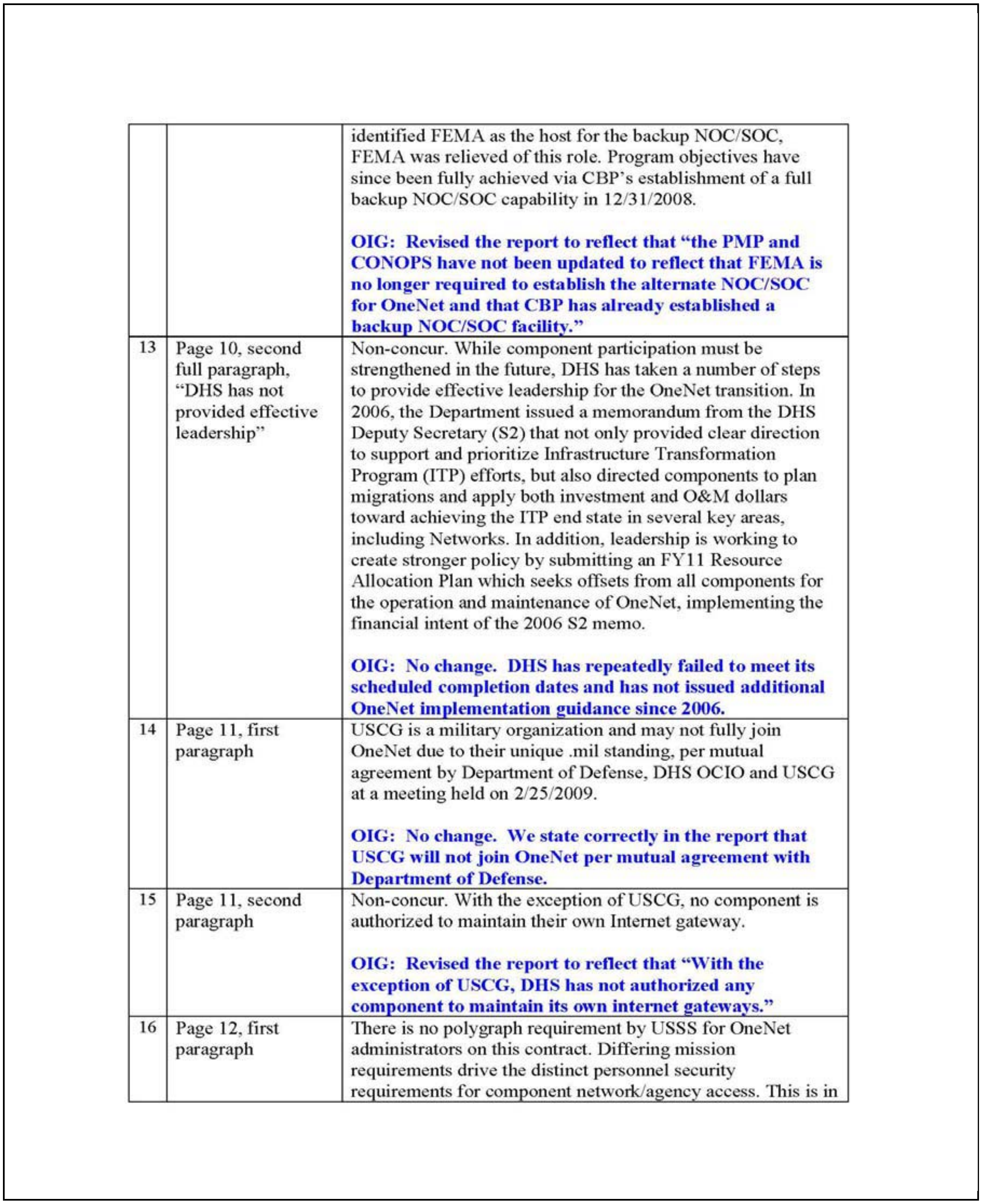
#	Report Section	DHS Comment
1	P. 1, second paragraph, "DHS has not provided effective oversight or leadership…to guide components' transition"	Non-concur. In addition to a strong leadership team that maintains day-to-day oversight, DHS has a multi-faceted structure in place to oversee and govern the OneNet program. The Interim Change Control Board (ICCB) assures that all changes are planned, engineered, tested, coordinated and approved prior to their release into the OneNet production environment; the Chief Information Security Officer (CISO) monitors performance of the Security Operations Center (SOC) to ensure SOC operations are compliant with CISO policies; the Senior Infrastructure Officer Council (SIOC) regularly reviews all current projects, schedule, cost and performance; and the Chief Information Officer Council, develops overarching guidance and directs the effort. At the CIO level, the DHS CIO/Deputy CIO and CBP CIO/Deputy CIO have frequent discussions regarding status of the OneNet implementation. In addition, at the program level, a number of reporting mechanisms are in place including monthly program management reviews with the DHS CIO covering cost, schedule and performance status. **OIG: Revised the report to clarify that "…DHS has not provided effective oversight or leadership to guide components' transition into OneNet and to ensure the completion of critical tasks for the consolidation."**
2	P. 1, third paragraph, "DHS does not have sufficient disaster recovery capability at its backup facility"	Non-concur. On 12/31/2008, DHS achieved Full Operating Capability of the backup Network Operations Center (NOC)/SOC facility. OneNet has fully redundant NOC/SOC server facilities with full live data replication in real-time, as well as live 24x7 NOC/SOC staff currently integrated in real time operations. OneNet and the backup NOC/SOC in [redacted] performed a successful Continuity of Operations (COOP) failover test in 01/2009 that included restoration and failover of all critical NOC and SOC applications to the backup NOC/SOC. **OIG: Revised the report to clarify that "..DHS does not have [redacted] to provide [redacted] at its backup facility."**
3	P. 7, "OneNet implementation is behind schedule"	There was a significant external factor in the late award of the GSA Networx Universal IDIQ contract, and the six month processing time for the DHS fair opportunity decision. In addition, DHS made a business decision to divert resources from the implementation in order to fully address OMB's



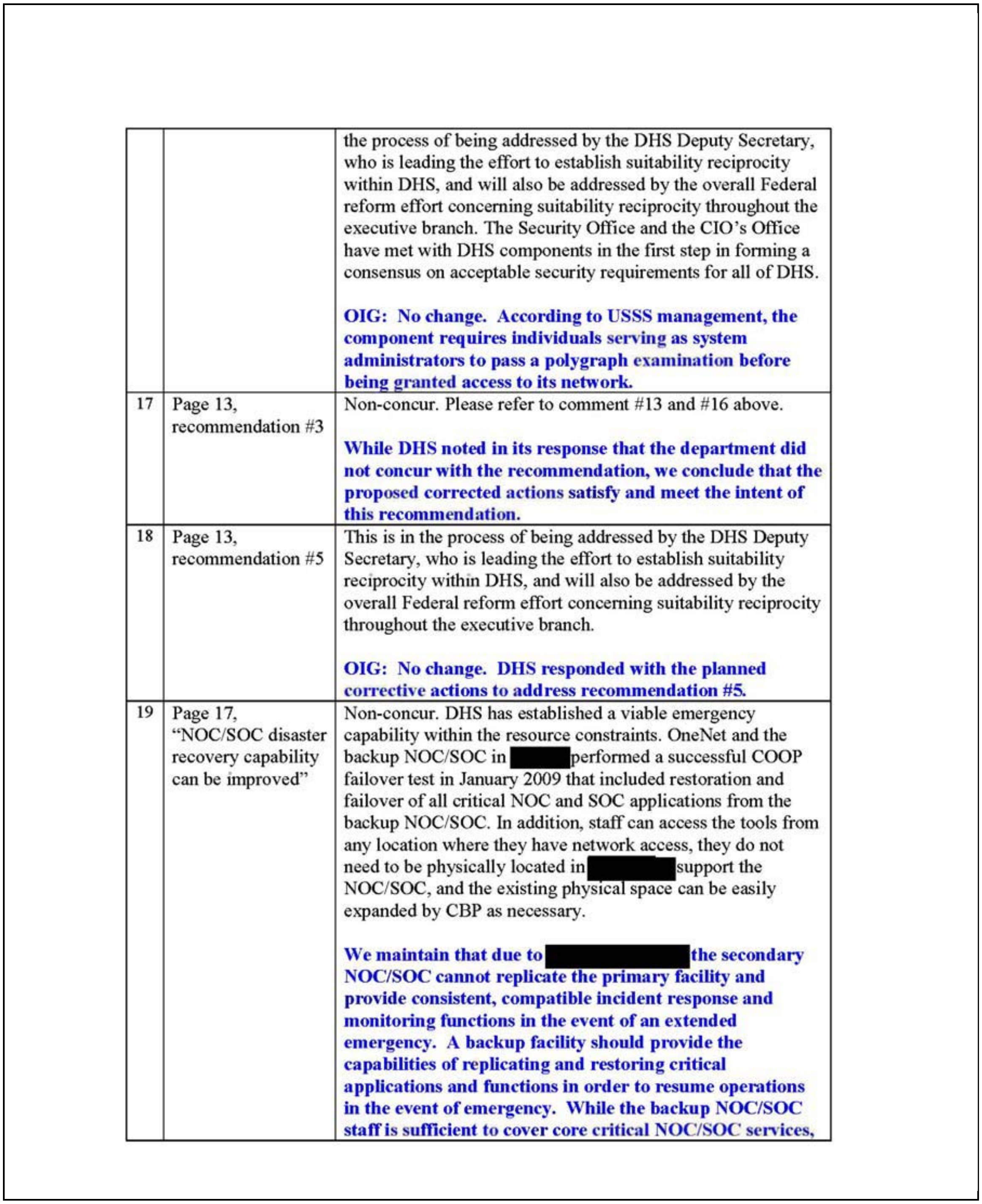
		Trusted Internet Connection (TIC) initiative. Additional time was also incurred in order to accomplish emerging component security requirements. **OIG: No change. DHS' delay in consolidating components' infrastructures into OneNet could not have been caused by GSA Networx contract. Specifically, DHS began its OneNet consolidation in July 2005 and OMB did not require agencies to use Networx contract until August 2008.**
4	Page 7, first full paragraph	Non-concur. Please refer to comment #1 above. **OIG: No change. We maintain that DHS has not provided effective oversight of components to ensure the timely implementation of OneNet or to guide components in their transition to DHS TIC. DHS must strengthen its oversight in order to reach its ultimate goal of consolidating and modernizing its existing infrastructure and achieve projected cost savings.**
5	Page 7, first bullet	Non-concur. DHS has achieved cost savings through this transition, and will accrue additional savings in the future as the OneNet transition is completed. Activities to date that have resulted in cost savings include: moving traffic from the [redacted] the collapse of ICE's hierarchical network, and the shut down of the TSA data center and the large bandwidth circuits associated with that data center. **OIG: Modified the report to clarify that the statement cited was from DHS' 2007 budget as the department had anticipated significant cost savings would be achieved by shutting down redundant networks at components after the consolidation.**
6	Page 7, firsts paragraph below the bullets	Non-concur. DHS anticipates a significant reduction in workload at component NOCs/SOCs, as work associated with the Wide Area Network (WAN) migrates to the Department. Component NOC/SOC functions will be reduced to Local Area Network (LAN) oversight, which remains outside of OneNet and within component responsibility. **OIG: No change. Although the department had anticipated in its 2007 budget that significant cost savings would be achieved by shutting down redundant networks at components after the consolidation, ITP program officials and CBP personnel do not foresee that any component networks will be shut down.**



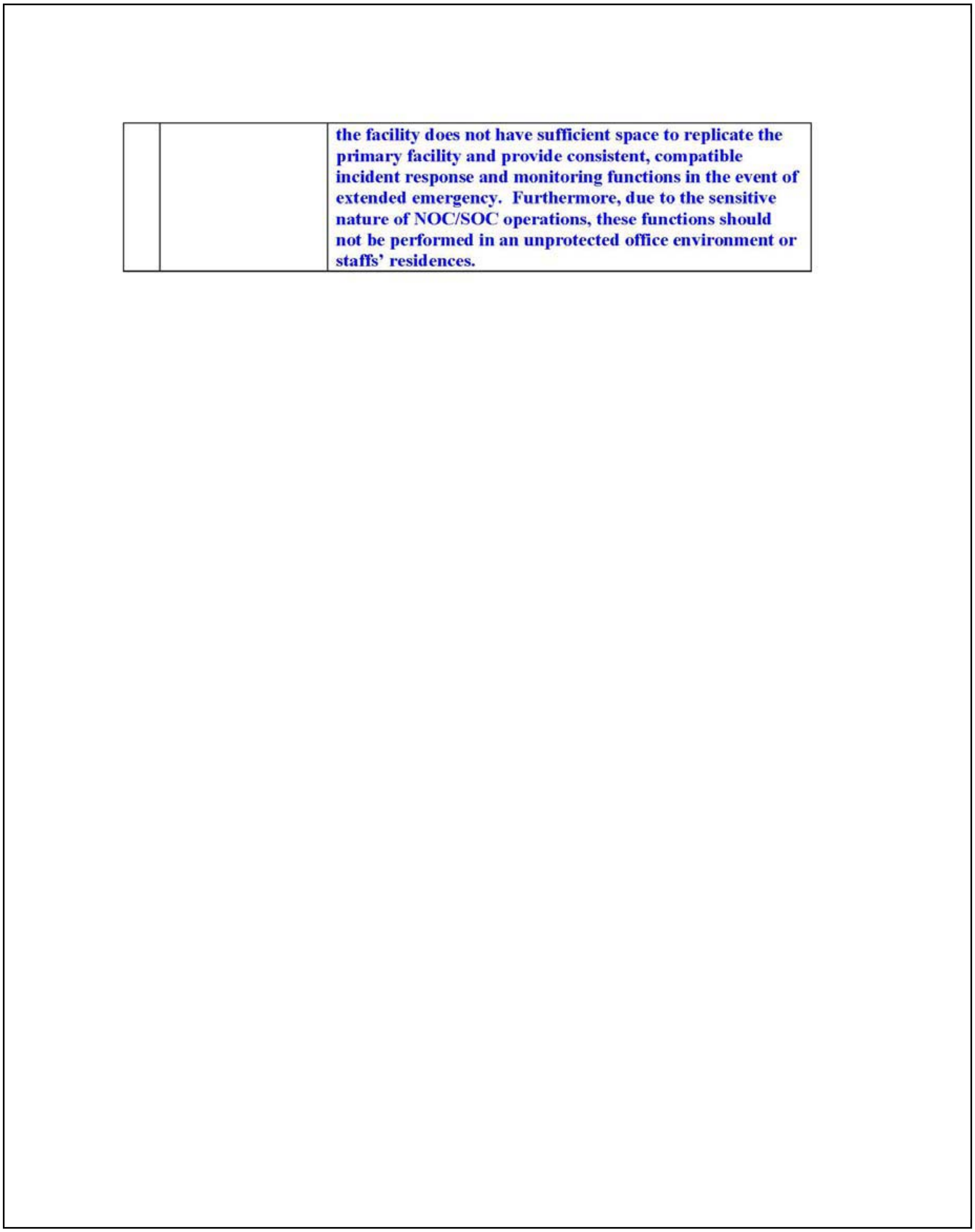
7	Page 7, first paragraph below the bullets "ITP program officials and CBP personnel do not foresee that any component networks will be shut down"	Non-concur. All component WANs will be subsumed by OneNet, with the exception of the United States Coast Guard (USCG). USCG will remain under governance of Defense Information Systems Agency (DISA). USCG is a military organization and will not fully join OneNet due to their unique .mil standing, per mutual agreement by Department of Defense, DHS OCIO and USCG in a meeting held on 2/25/2009. **OIG: No change. Once all component WANs are subsumed by or incorporated into OneNet , these networks will be managed by CBP. Components will still be responsible for managing their existing local area networks. As such, the statement "ITP program officials and CBP personnel do not foresee that any component networks will be shut down" is accurate. Furthermore, whether USCG will be under DISA governance has no effect on statement in report.**
8	Page 8, first paragraph, "target completion date of September 30, 2014"	Non-concur. The OneNet transition is on schedule for completion of its major components by early 2011. The FY10 budget request includes funds through 2014 for network sustainment (O&M), network enhancements and technology refresh. **OIG: Deleted statement referenced to DHS' FY2010 budget.**
9	Page 8, bullet at the bottom of the page	Non-concur. Phase I of the transition is complete, as all DHS Communications Network (DCN) circuit upgrades to [redacted] are complete. While the FEMA and USSS network conversions to [redacted] are still ongoing, these transitions are separate from the completion of Phase I conversion of the DCN to [redacted]. **OIG: Statement deleted.**
10	Page 9, first bullet, "ICE has not converted all of its sites to MPLS"	Non-concur. ICE has converted all sites to [redacted] where [redacted] services are available. In addition, all ICE circuits are under DHS NOC management. **OIG: Statement deleted.**
11	Page 9, second bullet "DHS has not completed Phase 1…therefore Phase III is not complete"	Non-concur. Phase I of the transition was completed as described in comment #9 above. In addition, no dependencies exist between the completion of Phase I and Phase III. Phase III is complete for the components identified in the report. **OIG: Statement deleted.**
12	Page 9, third bullet	Non-concur. While original Program Management Plan



		identified FEMA as the host for the backup NOC/SOC, FEMA was relieved of this role. Program objectives have since been fully achieved via CBP's establishment of a full backup NOC/SOC capability in 12/31/2008. **OIG: Revised the report to reflect that "the PMP and CONOPS have not been updated to reflect that FEMA is no longer required to establish the alternate NOC/SOC for OneNet and that CBP has already established a backup NOC/SOC facility."**
13	Page 10, second full paragraph, "DHS has not provided effective leadership"	Non-concur. While component participation must be strengthened in the future, DHS has taken a number of steps to provide effective leadership for the OneNet transition. In 2006, the Department issued a memorandum from the DHS Deputy Secretary (S2) that not only provided clear direction to support and prioritize Infrastructure Transformation Program (ITP) efforts, but also directed components to plan migrations and apply both investment and O&M dollars toward achieving the ITP end state in several key areas, including Networks. In addition, leadership is working to create stronger policy by submitting an FY11 Resource Allocation Plan which seeks offsets from all components for the operation and maintenance of OneNet, implementing the financial intent of the 2006 S2 memo. **OIG: No change. DHS has repeatedly failed to meet its scheduled completion dates and has not issued additional OneNet implementation guidance since 2006.**
14	Page 11, first paragraph	USCG is a military organization and may not fully join OneNet due to their unique .mil standing, per mutual agreement by Department of Defense, DHS OCIO and USCG at a meeting held on 2/25/2009. **OIG: No change. We state correctly in the report that USCG will not join OneNet per mutual agreement with Department of Defense.**
15	Page 11, second paragraph	Non-concur. With the exception of USCG, no component is authorized to maintain their own Internet gateway. **OIG: Revised the report to reflect that "With the exception of USCG, DHS has not authorized any component to maintain its own internet gateways."**
16	Page 12, first paragraph	There is no polygraph requirement by USSS for OneNet administrators on this contract. Differing mission requirements drive the distinct personnel security requirements for component network/agency access. This is in

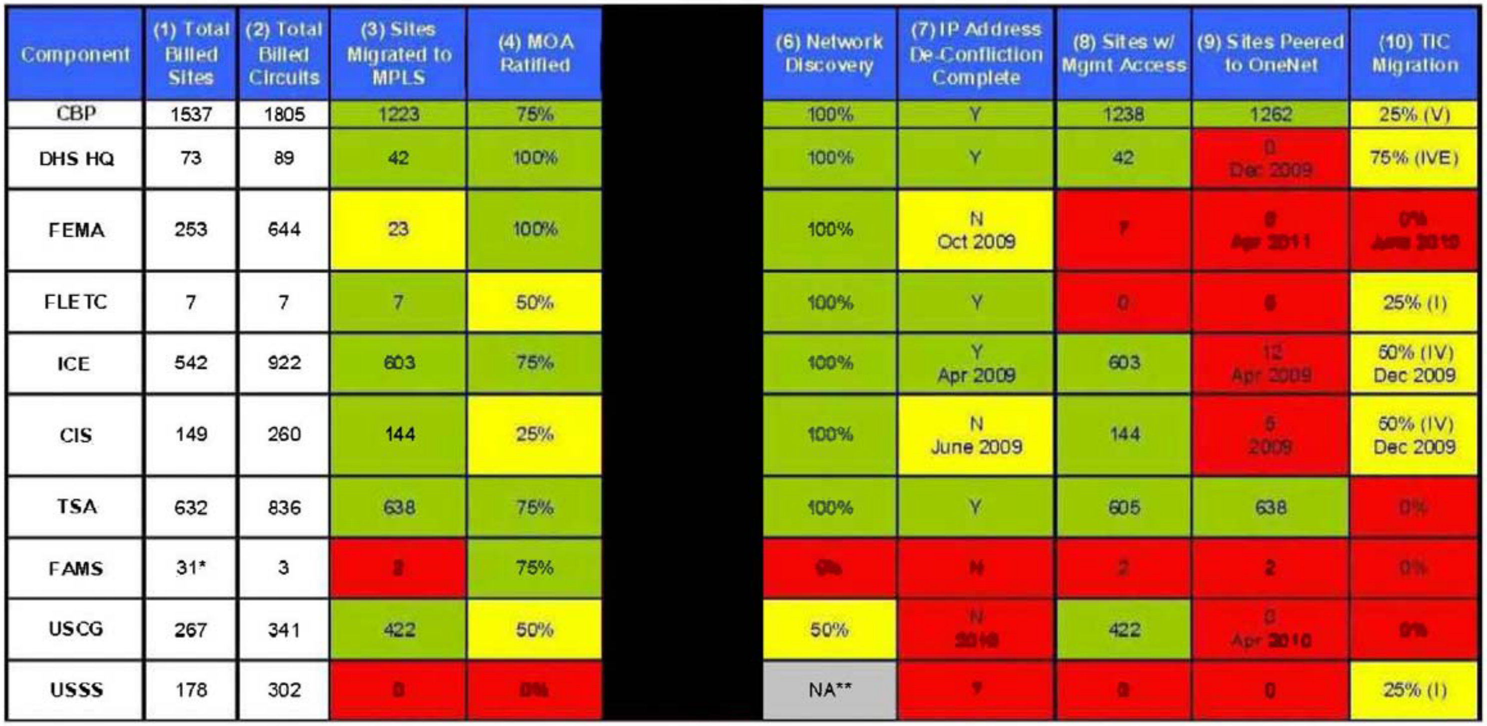


		the process of being addressed by the DHS Deputy Secretary, who is leading the effort to establish suitability reciprocity within DHS, and will also be addressed by the overall Federal reform effort concerning suitability reciprocity throughout the executive branch. The Security Office and the CIO's Office have met with DHS components in the first step in forming a consensus on acceptable security requirements for all of DHS. **OIG: No change. According to USSS management, the component requires individuals serving as system administrators to pass a polygraph examination before being granted access to its network.**
17	Page 13, recommendation #3	Non-concur. Please refer to comment #13 and #16 above. **While DHS noted in its response that the department did not concur with the recommendation, we conclude that the proposed corrected actions satisfy and meet the intent of this recommendation.**
18	Page 13, recommendation #5	This is in the process of being addressed by the DHS Deputy Secretary, who is leading the effort to establish suitability reciprocity within DHS, and will also be addressed by the overall Federal reform effort concerning suitability reciprocity throughout the executive branch. **OIG: No change. DHS responded with the planned corrective actions to address recommendation #5.**
19	Page 17, "NOC/SOC disaster recovery capability can be improved"	Non-concur. DHS has established a viable emergency capability within the resource constraints. OneNet and the backup NOC/SOC in [redacted] performed a successful COOP failover test in January 2009 that included restoration and failover of all critical NOC and SOC applications from the backup NOC/SOC. In addition, staff can access the tools from any location where they have network access, they do not need to be physically located in [redacted] support the NOC/SOC, and the existing physical space can be easily expanded by CBP as necessary. **We maintain that due to [redacted] the secondary NOC/SOC cannot replicate the primary facility and provide consistent, compatible incident response and monitoring functions in the event of an extended emergency. A backup facility should provide the capabilities of replicating and restoring critical applications and functions in order to resume operations in the event of emergency. While the backup NOC/SOC staff is sufficient to cover core critical NOC/SOC services,**



		the facility does not have sufficient space to replicate the primary facility and provide consistent, compatible incident response and monitoring functions in the event of extended emergency. Furthermore, due to the sensitive nature of NOC/SOC operations, these functions should not be performed in an unprotected office environment or staffs' residences.

Appendix C
Components' OneNet Implementation Status



Component	(1) Total Billed Sites	(2) Total Billed Circuits	(3) Sites Migrated to MPLS	(4) MOA Ratified	[redacted]	(6) Network Discovery	(7) IP Address De-Confliction Complete	(8) Sites w/ Mgmt Access	(9) Sites Peered to OneNet	(10) TIC Migration
CBP	1537	1805	1223	75%	[redacted]	100%	Y	1238	1262	25% (V)
DHS HQ	73	89	42	100%	[redacted]	100%	Y	42	0 Dec 2009	75% (IVE)
FEMA	253	644	23	100%	[redacted]	100%	N Oct 2009	7	0 Apr 2011	0% June 2010
FLETC	7	7	7	50%	[redacted]	100%	Y	0	0	25% (I)
ICE	542	922	603	75%	[redacted]	100%	Y Apr 2009	603	12 Apr 2009	50% (IV) Dec 2009
CIS	149	260	144	25%	[redacted]	100%	N June 2009	144	5 2009	50% (IV) Dec 2009
TSA	632	836	638	75%	[redacted]	100%	Y	605	638	0%
FAMS	31*	3	2	75%	[redacted]	0%	N	2	2	0%
USCG	267	341	422	50%	[redacted]	50%	N 2010	422	0 Apr 2010	0%
USSS	178	302	0	0%	[redacted]	NA**	Y	0	0	25% (I)

Appendix D
Major Contributors to this Report

Information Security Audit Division

Edward Coleman, Director
Chiu-Tong Tsang, Audit Manager
Mike Horton, IT Officer
Barbara Bartuska, Audit Manager
Maria Rodriguez, Team Lead
Aaron Zappone, Program Analyst
Nazia Khan, IT Specialist

Domingo Alvarez, Referencer

Appendix E
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Acting General Counsel
Executive Secretary
Assistant Secretary for Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Chief Information Officer
Deputy Chief Information Officer
Chief Information Security Officer
Director, Compliance and Oversight
Director, GAO/OIG Liaison Office
CIO Audit Liaison
Chief Information Security Officer Audit Manager

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.