

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Management of the
DHS Wide Area Network
Needs Improvement



Office of Information Technology

OIG-06-20

December 2005



**Homeland
Security**

Preface

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

This report assesses the processes and procedures for network monitoring, risk reduction, and incident reporting activities for the DHS wide area network communications system. 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. It is our hope that 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.

A handwritten signature in cursive script that reads "Richard L. Skinner".

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Executive Summary	1
Background.....	2
Results of Audit	4
Network Monitoring and Risk Reduction Activities Are Not Effective.....	4
Recommendations.....	10
Capital Planning Processes for the DHS Wide Area Network Need Improvement	11
Recommendation	13

Appendices

Appendix A: Purpose, Scope, and Methodology	15
Appendix B: Management’s Response to Draft Report	17
Appendix C: Security Event Messages from the DHS Wide Area Network.....	20
Appendix D: Top Sources for Most Security Event Messages.....	23
Appendix E: Top Sources for ‘ids.detect.misuse.porn’ Security Event Messages..	24
Appendix F: OneNetwork Timeline.....	25
Appendix G: Major Contributors to Report	26
Appendix H: Report Distribution.....	27

Abbreviations

ATM	Asynchronous Transfer Mode
C&A	Certification and Accreditation
CBP	Customs and Border Protection
CFO	Chief Financial Officer
CIO	Chief Information Officer
DHS	Department of Homeland Security
ICE	Immigration and Customs Enforcement
IP	Internet Protocol
IRB	Investment Review Board
ISA	Interconnection Service Agreement
IT	Information Technology
ITP	Infrastructure Transformation Program
MPLS	Multi-Protocol Label Switching
MRC	Management Review Council

Table of Contents/Abbreviations

NIST SP	National Institute of Standards and Technology Special Publication
OCIO	Office of Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget



*Department of Homeland Security
Office of Inspector General*

Executive Summary

We audited the Department of Homeland Security (DHS) and its Office of the Chief Information Officer (OCIO) to determine whether the security operations center for the DHS wide area network was performing its network monitoring, risk reduction, and incident reporting activities effectively. Also, in response to a request from the DHS Chief Information Officer (CIO) to include a review of changes being made to the DHS wide area network, we evaluated DHS' upgrade to the wide area network to determine if it complied with capital planning and investment control requirements. This audit included a review of applicable DHS and OCIO security policies, procedures, and other appropriate documentation. Last, we reviewed network security reports to evaluate the effectiveness of network monitoring procedures.

DHS implemented a wide area network to connect the separate legacy network infrastructures of the 22 organizations that were combined to form DHS. The DHS wide area network requires operational oversight and management to keep it functioning, and to respond to any service disruptions or security-relevant events that arise. One such information security component that provides network oversight and management is a security operations center.

The OCIO did not use automated network security tools for the DHS wide area network effectively to identify the cause of a growing number of automated security event messages. Our analysis of network security software databases identified several devices within DHS that were generating millions of security event messages each month. However, DHS had not finalized procedures for identifying the source of those messages or for coordinating appropriate actions with other technical and security organizations. DHS systems and data are at increased risk - of service disruptions and security-related events - if automated network security tools are not utilized effectively.

These problems were occurring in part because the DHS CIO had not established a security operations center for the DHS wide area network, but instead relied on the Immigration and Customs Enforcement (ICE) security operations center to perform the necessary network monitoring and risk reduction activities. Additionally, the roles and responsibilities of ICE staff performing these activities, and their interactions with DHS OCIO staff, were not documented. This informal collaboration between ICE and the OCIO to perform DHS security operations center activities places the DHS wide area network, and the subnets attached to it, at increased risk of service disruptions and security-related events.

In addition, the CIO did not follow DHS information technology (IT) capital planning and investment control processes for the selection and control of the DHS wide area network. Specifically, the CIO had implemented and operated the DHS wide area network for two years before issuing an “Interim Authority To Operate.”¹ Also, an upgrade to the DHS wide area network was selected and implemented without proper authorization. The DHS wide area network communication system and upgrades may include technical vulnerabilities - and may be subject to cost and schedule overruns - when DHS IT capital planning guidelines are not followed.

Background

DHS relies on a variety of critical IT systems and technologies to support its wide-ranging missions including counter-terrorism, border security, immigration, and infrastructure protection. DHS IT systems allow employees to communicate internally and for the American public to communicate with the department as well. One of these communication systems, the DHS wide area network, connects the separate legacy wide area networks of the 22 organizations that were combined to form DHS.² The DHS wide area network provides the infrastructure for its components to communicate internally and externally with partners and the public.

¹ Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, requires that a management official authorize in writing the use of general support systems, such as wide area networks, based on implementation of its security plan before beginning processing in the system.

² The DHS wide area network, initially called the DHS Core Network, is comprised of (1) two major Internet Data Centers; (2) the Asynchronous Transfer Mode (ATM) circuits that connect the two Internet Data Centers to each other and to the large DHS wide area networks and data centers; and, (3) the frame relay circuits which are used to connect smaller wide area networks to the two Internet Data Centers.

The DHS wide area network was implemented in a short time frame during the creation of DHS in order to connect the various components of the new department. OCIO personnel consider the initial DHS wide area network to be a temporary arrangement. OCIO staff has been upgrading the original Asynchronous Transfer Mode- (ATM-) and frame relay-based DHS wide area network into the “OneNetwork” infrastructure, a domain-based network using the Multi-Protocol Label Switching (MPLS) as the transport technology. Upgrading the DHS wide area network to enable MPLS capability is the first phase of the OneNetwork implementation.

A typical security operations center should be responsible for managing the configuration, operation, monitoring, and maintenance of security devices deployed throughout a network, and to document and pursue all reported network, server, and desktop security incidents. In fulfilling these responsibilities, a security operations center needs to collect data, such as security event messages, from firewalls and other devices. Performance of security operations center activities for the communications system connecting its organizational components is an essential component of the DHS IT security program.

A security operations center then analyzes the event data to determine if a possible security incident has occurred.³ Security incidents that a security operations center determines to be significant are to be passed to a computer security incidence response center (a separate organization) for further response coordination.⁴

³ National Institute of Standards and Technology Special Publication (NIST SP) 800-61, *Computer Security Incident Handling Guide*, defines an event as “any observable occurrence in a system or network.” Some examples of events include a:

- User connecting to a file share
- Server receiving a request for a Web page
- User sending e-mail
- Firewall blocking a connection attempt

Adverse events are events with negative consequences, such as system crashes, unauthorized use of system privileges, failure of a critical security device (such as a firewall), or execution of malicious code that destroys data. An incident, formerly limited to a security related adverse event, is now described in NIST SP 800-61, as “a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.” Some examples of incidents are:

- Denial of Service (DoS): An attacker sends specially-crafted packets to a server, causing it to crash, or directs numerous compromised computers in a distributed-denial-of-service attack on an organization.
- Execution of Malicious Code: A virus propagates through e-mail, infecting recipients’ computers with malicious code, or a worm uses open file shares to infect numerous computers within an organization.
- Attainment of Unauthorized Access: An attacker runs an exploit tool, gaining access to a server’s password file, or obtains unauthorized administrator-level access.

⁴ The ICE computer security incident response center is also performing computer security incident response center activities for the DHS OCIO.

Technologies that a security operations center could employ for the collection and analysis of data include intrusion detection systems, and security incident management systems. Intrusion detection system products are designed to identify suspicious events and record pertinent data, including the date and time the attack was detected, the type of attack, the source and destination Internet Protocol (IP) addresses, and the username (if applicable and known). A security incident management system automates the collection of security event messages, logs, and other data from a wide set of sources, including firewalls and intrusion detection systems.

The large number of security event messages that are often generated makes it difficult to discern those that indicate an adverse event or even that a computer security incident has occurred and must be addressed.⁵ A security incident management system provides meaningful security information, via reports and a centralized console, to help security operations center personnel identify security incidents and respond to events that may cause harm to the system.

Results of Audit

Network Monitoring and Risk Reduction Activities Are Not Effective

The OCIO is not using network security software to identify the cause of a growing number of automated security event messages. OCIO and ICE were not performing network monitoring and risk reduction activities effectively because the DHS CIO had not established a security operations center for the DHS wide area network. DHS decided not to address security management issues on the DHS wide area network because it was planning to transform the network to the OneNetwork infrastructure. In doing so, it left the DHS wide area network subject to increased risk of service disruptions and security-related events.

Ineffective Network Monitoring

OCIO does not have a standard methodology for analyzing the security event messages and is not blocking external web sites that

⁵ For example, according to NIST SP 800-61, a single Web vulnerability scan against one Web server can generate hundreds of alerts on both a network-based intrusion detection system and the Web server's host-based intrusion detection system product. An attacker performing such a scan on ten Web servers could generate several thousand intrusion detection system alerts.

were the source of some of these messages. While ICE staff monitored the DHS wide area network with a variety of tools and were capturing security event messages, they were not providing information on these messages to DHS computer security officials on a consistent basis.

In July 2004, prior to the start of our audit, approximately 5.4 million security event messages were generated each month by the DHS wide area network. At our entrance conference in November 2004, the DHS CIO requested that we provide a breakdown of the security event messages that were generated. We reviewed the security event messages generated by the DHS wide area network intrusion detection system in February, March, and April 2005 (the three months of security event messages are summarized in Appendix C). There were approximately 65 million messages generated during these three months. This average, of approximately 22 million messages a month, is more than a 400% increase in the monthly averages for security event messages as compared to the averages that occurred less than a year earlier.

During the three-month period reviewed, 16 devices generated approximately 45.5 million of the 65 million security event messages (70%) recorded on the DHS wide area network (see Appendix D). Approximately 6.5 million (10%) of the 65 million security event messages were the 'ids.detect.misuse.porn' message.⁶ Additionally, 4.9 million of the 6.5 million 'ids.detect.misuse.porn' messages (approximately 75%) were generated by 16 devices or web sites. (See Appendix E)

We provided a list of 45 devices and sites that were the source of large volumes of security event messages to ICE computer security incident response center staff.⁷ We requested information concerning the source that was generating the security event messages, including its location, the device type (such as workstation or server), the owner of the device, and what actions ICE had taken concerning these devices.

⁶ DHS policy forbids DHS employees from accessing pornographic material. Intrusion detection system sensors are programmed to look for pornographic related words, for example the word "oral". The 'ids.detect.misuse.porn' security event message would be generated when the intrusion detection system sensors detect one of these known words. However, this word might be present within other legitimate words, such as "behavioral" and, following a review of the event, may not require further action.

⁷ The list of 45 Internet Protocol (IP) addresses included those devices and web sites that generated a large number of messages, a large number of 'ids.detect.misuse.porn' messages, and a large number of different messages.

ICE could not identify the specific workstation that generated the messages. For example, due to the use of randomly generated IP addresses, ICE could only determine that the workstation was attached to a server whose IP address was in the generated messages. ICE could not demonstrate how it responded to security event messages generated by the IP address or whom they had contacted about those messages.

Additionally, we contacted our own IT staff concerning the security event messages generated by devices on our subnet. Our IT staff reported that they stored the logs of the randomly generated IP addresses for one week. Therefore, our IT staff could not identify the specific workstation that produced the messages unless they were contacted within one week after the security event messages were generated.

DHS systems and data are at increased risk of service disruptions and security-related events if automated network security tools are not utilized effectively. According to National Institute of Standards and Technology Special Publication (NIST SP) 800-61, *Computer Security Incident Handling Guide*, if security controls are insufficient high volumes of incidents may occur, overwhelming the resources and capacity for response, which would result in delayed or incomplete recovery - and possibly more extensive damage and longer periods of service or data unavailability.

NIST SP 800-61 requires that an effective incident response capability include:

- The continual monitoring of threats through intrusion detection system and other mechanisms;
- The establishment of clear procedures for assessing the current and potential business impact of incidents;
- The implementation of effective methods of collecting, analyzing, and reporting data; and,
- The building of relationships and establishing suitable means of communication with other internal groups, such as human resources and legal, and with external groups, including other incident response teams and law enforcement.

Additionally, NIST SP 800-61 recommends that agencies establish logging standards and procedures to ensure that logs and security software collect adequate information and that the data is reviewed

regularly. NIST SP 800-61 recommends that log data should be retained for at least a few weeks, preferably for at least a few months.

We discussed our concerns with staff from the OCIO and ICE. During these discussions, ICE staff pointed out that some of the sources of the messages were servers to which possibly thousands of computers could be attached. This scenario made it difficult to determine whether one computer was infected or the volume of messages generated was simply the result of the compilation of a small number of messages generated by a large number of computers. OCIO and ICE staff noted that some DHS law enforcement organizational components may be creating security event messages due to the content of their emails or due to the web sites they may be reviewing. Additionally, according to OCIO and ICE staff, the increase in security event messages may be a result of bringing more devices online and to increasing the type of events the DHS wide area network intrusion detection system was recording. While OCIO staff are concerned that setting a goal of reducing the number of security event messages may result in missing an adverse event, they agreed that they needed to focus on the large number of security event messages.

Informal Security Management Process

The CIO relies on an informal collaboration between the OCIO and ICE staff to perform security management activities for the DHS wide area network. The lack of a formal agreement between the OCIO and ICE places DHS at risk of not detecting an adverse incident, not being able to respond in a timely manner, and not being able to contain or minimize the damage to its IT systems.

The ICE security operations center is able to monitor the DHS wide area network and the ICE staff responds to requests from OCIO staff to perform network monitoring and other activities for the DHS wide area network. However, there was no documented agreement, or memorandum of understanding, between the OCIO and ICE formally tasking the ICE security operations center to perform these activities for the DHS wide area network. Further, the CIO had not issued policies or procedures assigning DHS security operations center security-related roles and responsibilities.

Finally, there was no formal memorandum of understanding detailing the required interaction between ICE staff performing

DHS security operations center activities and other technical and security organizations, including a DHS computer security incident response center, or the contractors maintaining the DHS wide area network firewalls.

Interconnection Service Agreements

The OCIO did not establish interconnection service agreements (ISA) with DHS components prior to connecting their systems to the DHS wide area network.⁸ ISAs document security protections - such as agreed upon baseline security controls and rules of use on the interconnected systems - to ensure only acceptable transactions are permitted. We determined that six DHS organizational components did not have ISAs for their wide area networks connected to the DHS wide area network.⁹ Other ISAs that we reviewed were obsolete or will become invalid when the upgraded DHS wide area network starts using the MPLS capability.¹⁰ Additionally, many of the references cited in the existing ISAs need to be updated to reflect the latest DHS standards and procedures.

ISAs for connection to the DHS wide area network should control access to and from other systems, as well as place limitations on outside access. For example, DHS law enforcement organizational components may be accessing suspect Internet sites in the course of their investigations. However, accessing these suspect sites through the DHS wide area network could be producing numerous security event messages and may place the DHS wide area network, and attached subnets, at risk. Without ISAs and rules of behavior, the OCIO cannot remove the offending subnet from the DHS wide area network, or require that this work be performed in a manner that minimizes risk, such as through a dial-up line.

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, requires written authorization, based upon the acceptance of risk to the system, prior to connecting a wide area network with other systems. OMB

⁸ DHS Sensitive Systems Policy Publication 4300A, *Information Technology Security Program*, requires components to document interconnections with other networks with an ISA.

⁹ CBP, Customs and Immigration Services, ICE, Transportation Security Administration, United States Coast Guard, and the United States Secret Service.

¹⁰ The following organizations have ISAs for their connection to the DHS wide area network: Federal Emergency Management Agency, Lawrence Livermore National Laboratory, Sandia National Laboratories, the legacy Critical Infrastructure Assurance Office, Department of Energy, Agriculture Animal & Plant Health Inspection Service, the General Services Administration, the National Communications System, and the Office of Justice Programs.

Circular A-130 also requires that, where connection is authorized, controls shall be established that are consistent with the rules of the system. The rules shall also include appropriate limits on interconnections to other systems, define service provision and restoration priorities, and be clear about the consequences of behavior not consistent with the rules.

Network Security Improvements

OCIO staff agreed that they could not wait until the transformation to the OneNetwork infrastructure is complete before security related improvements are made. Additionally, during our audit fieldwork, OCIO staff took actions to increase security and management of the DHS wide area network and the OneNetwork to include:

- Appointment of an information systems security manager for the DHS wide area network.
- Preparation of a draft security plan for the OneNetwork infrastructure.
- Providing for separation of duties by assigning separate managers for the OneNetwork development and legacy DHS wide area network operations.
- Starting the certification and accreditation process for the OneNetwork infrastructure.
- Planning an information security risk assessment for OneNetwork infrastructure.
- Adding additional equipment to its standard DHS wide area network installation to provide improved and regular traffic analysis.

Recommendations

We recommend that the DHS CIO establish:

1. A formal security operations center for the DHS wide area network by assigning staff and creating the necessary policies, procedures, and contract task orders to perform the required network monitoring and risk reduction activities,
2. The required interconnection service agreements for those systems connected to the DHS wide area network, and
3. A process to share DHS wide area network security event messages information in a timely fashion with computer security officers for the subnets affected.

Management Comments and OIG Analysis

DHS concurs with the recommendations provided in the report and has implemented several specific actions to implement them.

Concerning recommendation number 1, DHS has established a program for the DHS OneNetwork. It consists of networks, e-mail, data centers, and video domains. Under the network domain, are the operational plans for network operations centers and security operations centers. The initial DHS network operations center/security operations center is in Lafayette, Colorado and is under the direction of the CIO's Director of Operations. This day-to-day operation is being transferred to the implementing component – U.S. Customs and Border Protection (CBP).

We agree that the steps that DHS has taken, and plans to take, are responsive to this recommendation.

Concerning recommendation 2, DHS noted that some ISAs for the wide area network are in place. Further, CBP, as the network steward, will establish, maintain, and update an ISA repository and will provide ISA status updates to the DHS CIO.

We agree that the steps that DHS has taken, and plans to take, are responsive to this recommendation.

Concerning recommendation number three, DHS commented that this was a valid issue at the time this report was drafted. DHS also stated that currently, the DHS security operations centers (SOC)

provides real-time security monitoring, intrusion detection, incident handling, and reporting to the Director of Operations on behalf of the DHS CIO.

We agree that the steps that DHS has taken, and plans to take, are partially responsive to this recommendation: DHS recognized the importance of incident handling, but did not state that security event information would be shared with the security officers for the affected subnets.

Capital Planning Processes for the DHS Wide Area Network Need Improvement

The CIO did not follow DHS IT capital planning and investment control processes when implementing the DHS wide area network. Further, DHS had not assessed the management, operational, and technical controls before or since the DHS wide area network was implemented. In addition, IT capital planning and investment control processes were ineffective in guiding the selection and implementation of the OneNetwork.

Network Lacks Certification and Accreditation

The initial DHS wide area network did not have required documentation submitted for certification and accreditation (C&A). Additionally, the DHS CIO had not formally authorized the initial DHS wide area network to operate and has not provided for the independent review of security of the network. As a result, the DHS wide area network operated without an approved security risk assessment, security plan, or C&A. The OCIO staff viewed the initial DHS wide area network as a temporary solution that was to be transformed into the OneNetwork infrastructure. Following the May 18, 2005 cut-over to the MPLS technology, OCIO staff renamed the DHS wide area network as the OneNetwork. Now they are focusing C&A activities on this OneNetwork infrastructure.

The CIO granted an interim authority to operate for the OneNetwork on April 12, 2005; however, this authorization was flawed because the OneNetwork did not meet DHS baseline security requirements. Without performing security reviews and C&A activities, the OCIO cannot be assured that management, operational, personnel, and technical controls for the DHS wide area network are functioning effectively.

The DHS wide area network meets the definition of a general support system under OMB Circular A-130 and the DHS Sensitive Systems Policy Publication 4300A, *Information Technology Security Program*. OMB Circular A-130 requires that adequate security be provided for general support systems and that they include:

- Reviewing the security controls when significant modifications are made to the system, but at least every three years;
- Ensuring that a management official authorizes in writing the use of the system based on implementation of its security plan before beginning or significantly changing processing in the system; and
- Re-authorizing the use of the system at least every three years.

The OneNetwork Lacks Required Approvals

The OCIO had not received the required approval from the Investment Review Board (IRB) to implement the OneNetwork infrastructure.¹¹ However, by May 18, 2005, the implementation of the first phase of the OneNetwork infrastructure was completed (see Appendix F). This phase consisted of fitting all the DHS wide area network connections with the hardware and software to utilize the MPLS technology.

The project to transform the DHS wide area network into the OneNetwork infrastructure was included as the network portion of a larger OCIO project, the DHS Infrastructure Transformation Program (ITP). The DHS IRB had designated the ITP a Level 1 project. This designation required the ITP to be reviewed and approved by the DHS IRB, chaired by the Deputy Secretary. On March 11, 2005, the DHS Under Secretary for Management said that the ITP was not ready for review; the IRB did not approve this project for implementation.

On April 18, 2005, the OCIO submitted a request to the Management Review Council for approval to proceed with the implementation. On April 20, 2005, the acting Deputy CIO directed that a 45-day assessment of the ITP be performed. No

¹¹ The OCIO estimated that the fiscal year 2005 cost to implement the OneNetwork infrastructure would be \$28 million.

further approval actions were taken pending the completion of the assessments.

By not complying with its own investment policies, DHS risks spending on investments which may not directly support or further its mission, or provide optimal benefits to stakeholders and customers. Additionally, DHS cannot ensure that the DHS OneNetwork will have adequate security or be an appropriate investment if required risk assessments are not performed.

OMB Circular A-130 requires that agencies establish and maintain a capital planning and investment control process that links mission needs, information, and information technology in an effective and efficient manner. The DHS capital planning process is outlined in DHS Management Directive 1400, *Investment Review Process*. It includes DHS' efforts to ensure acquisition oversight of new investments throughout their life cycle and portfolio management to achieve budget goals and objectives. Management Directive 1400 categorizes DHS investments into levels and establishes the documentation required for review as well as the approval process for these capital investments.

We discussed these issues with OCIO staff who were unaware that they lacked the required approvals before proceeding with the first phase of the OneNetwork implementation. Additionally, the CIO required that the OneNetwork be fully authorized to operate by the expiration of the interim authority to operate. The OCIO is also performing the assessments required prior to the DHS IRB review and approval of the OneNetwork.

Recommendation

We recommend that the DHS CIO ensure that:

4. The OneNetwork undergoes certification and accreditation and is approved by the Investment Review Board before it is fully implemented across DHS.

Management Comments and OIG Analysis

DHS concurs with this recommendation and noted that the Deputy Secretary was briefed on July 26, 2005 with a resulting Program Decision document being signed on July 11, 2005. The DHS OneNetwork program is currently undergoing Key Decision Point reviews. As DHS OneNetwork becomes operational it will be accredited in accordance with DHS policy.

We agree that the steps that DHS has taken are responsive to this recommendation. Further, the steps that DHS plans to take are responsive provided that the DHS OneNetwork is accredited before it is fully implemented.

Purpose, Scope, and Methodology

The objective of this audit was to determine whether DHS' security operations center effectively performs its network monitoring, risk reduction, and incident reporting activities. Additionally, we planned to procure a contractor to perform an analysis of the DHS wide area network to determine if an improperly configured network infrastructure increased the risk of attacks and vulnerabilities to the DHS wide area network.

During our entrance conference, the DHS CIO requested that we (1) determine the types of security event messages that were being produced; (2) compete the network analysis procurement; and, (3) research the transformation of the DHS wide area network to the OneNetwork infrastructure.

In response to these requests, we did a more extensive review of the security event messages created on the DHS wide area network, including providing a breakdown of all the security event messages over a three-month period (see Appendix C). Also, we reviewed analysis and investment decisions related to the OneNetwork. Additionally, in response to the request to award the network analysis contract competitively, we identified several contractors who could perform the requested network analysis. However, we were unable to obtain a contractor in time to perform work during this audit. We accomplished this portion of our audit work by obtaining network analysis reports on the DHS wide area network from ICE and performing our own review of these reports.

We reviewed DHS policies, procedures and documentation, communications diagrams, security event messages, network management reports, and prior audit reports. We interviewed key government and contractor personnel, too. Fieldwork was performed at DHS and ICE facilities in the Washington, DC area and at the ICE security operations center.

We provided the OCIO with briefings concerning the results of fieldwork, including network analysis and security event messages information as well as the information summarized in this report.

We conducted this audit between November 2004 and July 2005. We performed our work according to generally accepted

government auditing standards and pursuant to the Inspector General Act of 1978, as amended.

We appreciate the efforts by DHS management and staff to provide the information and access necessary to accomplish this audit. The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General for Information Technology (202) 254-4100 and Roger Dressler, Director for Information Systems and Architectures (202) 254-5441. Major OIG contributors to the audit are identified in Appendix G.

Appendix B
Management's Response to Draft Report



**Homeland
Security**

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

December 9, 2005

MEMORANDUM FOR: Richard Skinner,
Inspector General, DHS

FROM: Scott Charbo
Chief Information Officer, DHS 

SUBJECT: Management Response to Draft Audit Report,
*Management of the DHS Wide Area Network Needs
Improvement (A-IT-05-004)*

Thank you for the opportunity to respond to the recommendations contained in the subject report. The recommendations you provided are well-considered and are consistent with our plans. The Department of Homeland Security (DHS) Office of the Chief Information Officer (CIO) concurs with the recommendations provided in the report and have implemented several specific actions to address them. Below is DHS' Management Response.

OIG RECOMMENDATION # 1 - *The DHS CIO establish a formal security operations center for the DHS wide area network by assigning staff and creating necessary policies, procedures, and contract task orders to perform the required network monitoring and risk reduction activities.*

DHS RESPONSE: The Office of the Chief Information Officer (CIO) has established a program for Department of Homeland Security OneNet. It consists of networks, e-mail, data centers, and video. Under the network domain, are the operational plans for network operations centers (NOC) and security operations centers (SOC.) The initial Department of Homeland Security NOC/SOC is in Lafayette, Colorado and is under the direction of the CIO's Director of Operations. This day-to-day operation is being transferred to the implementing component – U.S. Customs and Border Protection (CBP).

As we build out the OneNet core, Departmental-wide capabilities will be stood up. DHS OneNet is in the process of being constructed and, subject to funding, is scheduled to be completed by December 1, 2006.

Appendix B
Management's Response to Draft Report

DHS Response on WAN Report
Page 2 of 3

OIG RECOMMENDATION #2 - *The DHS CIO establish the required interconnection service agreements for those systems connected to the DHS wide area network.*

DHS RESPONSE: The DHS Office of the Chief Information Officer concurs with the OIG recommendation. Some Interconnectivity Security Agreements (ISA) for the wide area network are in place. U.S. Customs and Border Protection (CBP), as the network steward, will establish, maintain, and update an ISA repository and will provide ISA status updates to the DHS CIO.

OIG RECOMMENDATION #3 - *The DHS CIO establish a process to share DHS wide area network security event messages information in a timely fashion with computer security officers for the subnets affected.*

DHS RESPONSE: We recognize that this was a valid issue at the time this report was drafted. Currently, the DHS security operations centers (SOC) provides real-time security monitoring, intrusion detection, incident handling, and reporting to the Director of Operations on behalf of the DHS CIO.

OIG RECOMMENDATION #4 - *The OneNetwork undergoes certification and accreditation and is approved by the Investment Review Board before it is fully implemented across DHS.*

DHS RESPONSE: The Department of Homeland Security (DHS) Infrastructure Transformation Program (ITP) which oversees DHS OneNet was briefed to the Deputy Secretary on July 26, 2005 with a resulting Program Decision document being signed on July 11, 2005. The One Net program is currently undergoing KDP 2 / KDP 3 (interim) review. Key Decision Point (KDP) reviews are points at which the appropriate DHS review authority determines if and when an investment receives approval to reach the next phase. As OneNet becomes operational it will be accredited in accordance with DHS policy. For informational purposes, the KDP levels are as follows:

- **KDP 0: Program Initiation Phase** – Components and program/project managers are responsible for conducting ongoing operational analysis.
- **KDP 1: Concept and Technology Development Phase** – The focus is on setting technical requirements and exploring alternative solutions for meeting mission and operational needs.

Appendix B
Management's Response to Draft Report

DHS Response on WAN Report
Page 3 of 3

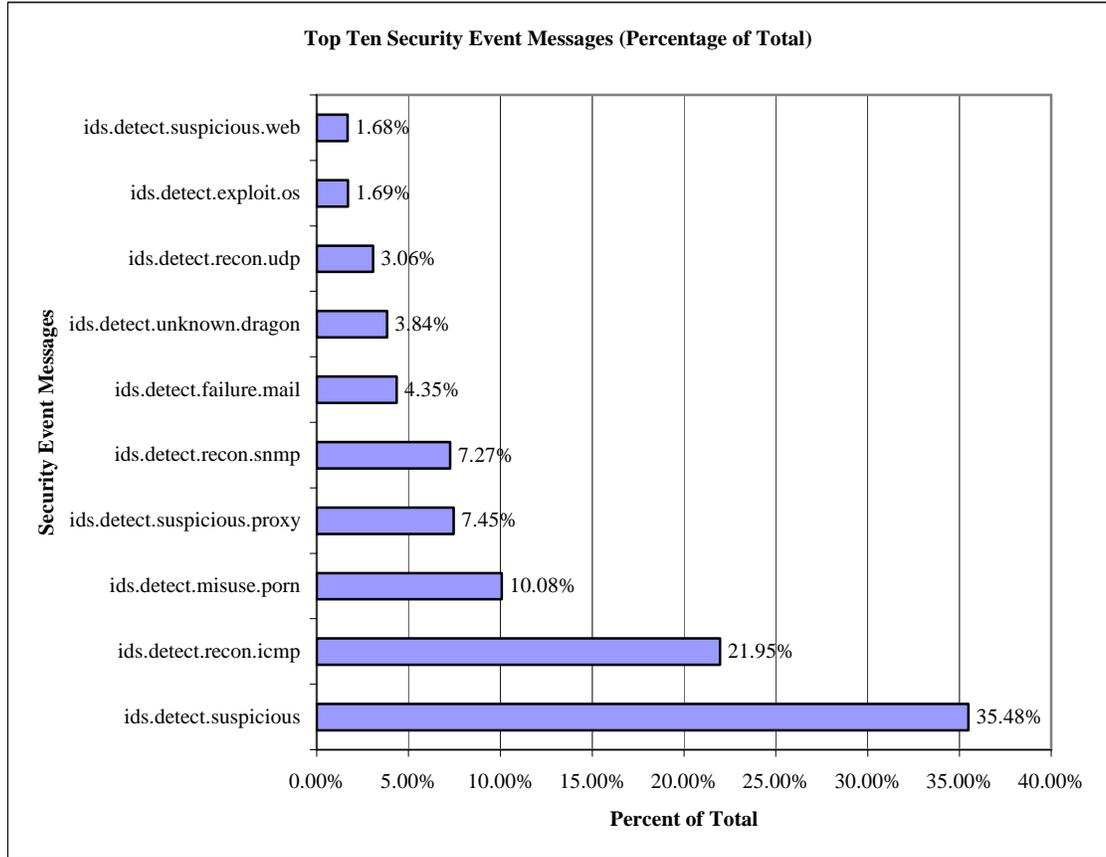
- KDP 2: Capability Development & Demonstration Phase - The focus is on demonstrating feasibility of the preferred alternative and refining the solution prior to a full production commitment.
- KDP 3: Production and Deployment Phase - The objective is to produce systems and equipment for deployment into operational use, in an effort to achieve full operational capability that satisfies the mission need.
- KDP 4: Operational and Support Phase - The objective is to use the asset to perform required missions. Reviews are conducted to ensure the asset is meeting performance and cost goals.

#

Appendix C
Security Event Messages from the DHS Wide Area Network

Security Event Messages from the DHS Wide Area Network for
February, March, and April 2005.

Security Event Message	Number of Messages	% of Total	Security Event Message	Number of Messages	% of Total
ids.detect.suspicious	23,078,318	35.48%	ids.detect.info.auth	5,783	0.01%
ids.detect.recon.icmp	14,279,625	21.95%	ids.detect.recon.mail	4,597	0.01%
ids.detect.misuse.porn	6,556,209	10.08%	ids.detect.insecure.service	3,740	0.01%
ids.detect.suspicious.proxy	4,846,369	7.45%	ids.detect.recon	2,831	0.00%
ids.detect.recon.snmp	4,728,282	7.27%	ids.detect.dos.os	2,067	0.00%
ids.detect.failure.mail	2,828,033	4.35%	ids.detect.exploit.db	1,648	0.00%
ids.detect.unknown.dragon	2,495,864	3.84%	ids.detect.recon.backdoor	1,396	0.00%
ids.detect.recon.udp	1,993,017	3.06%	ids.detect.exploit.ftp	1,023	0.00%
ids.detect.exploit.os	1,101,747	1.69%	ids.detect.virus	1,019	0.00%
ids.detect.suspicious.web	1,093,848	1.68%	ids.detect.suspicious.net	875	0.00%
ids.detect.insecure.ftp	566,053	0.87%	ids.detect.auth.shell.login.deny	860	0.00%
ids.detect.recon.web	286,543	0.44%	ids.detect.worm	821	0.00%
ids.detect.insecure.web	271,320	0.42%	ids.detect.insecure.os	620	0.00%
ids.detect.exploit.web	199,692	0.31%	ids.detect.misuse.dos	446	0.00%
ids.detect.suspicious.snmp	154,790	0.24%	nsm.threshold.exceeded2	446	0.00%
ids.detect.auth.web.login.deny	124,010	0.19%	ids.detect.misuse.chat	346	0.00%
ids.detect.exploit.dns	104,260	0.16%	ids.detect.exploit.snmp	217	0.00%
ids.detect.suspicious.mail	82,697	0.13%	ids.detect.deny.service	144	0.00%
ids.detect.compromise	36,109	0.06%	ids.detect.misuse.backdoor	75	0.00%
ids.detect.recon.dns	32,334	0.05%	ids.detect.dos.mgmt	49	0.00%
ids.detect.auth.login.web.deny	28,916	0.04%	ids.detect.exploit.net_mgmt	31	0.00%
ids.detect.suspicious.ftp	26,561	0.04%	ids.detect.recon.mgmt	22	0.00%
ids.detect.auth.ftp.login.deny	20,833	0.03%	ids.detect.exploit.groupware	11	0.00%
ids.detect.dos.web	18,634	0.03%	ids.detect.misuse.tool	8	0.00%
corr.xdevice	18,211	0.03%	ids.detect.dos.resources	7	0.00%
ids.detect.insecure.auth	12,232	0.02%	ids.detect.dos	6	0.00%
ids.detect.exploit.mail	9,418	0.01%	ids.detect.exploit.worm	4	0.00%
ids.detect.suspicious.icmp	7,020	0.01%	ids.detect.misuse.p2p	3	0.00%
ids.detect.fail.db	6,856	0.01%	ids.detect.misuse.warez	2	0.00%
ids.detect.misuse.jobs	6,438	0.01%			
			Total Num Events	65,043,336	100.00%

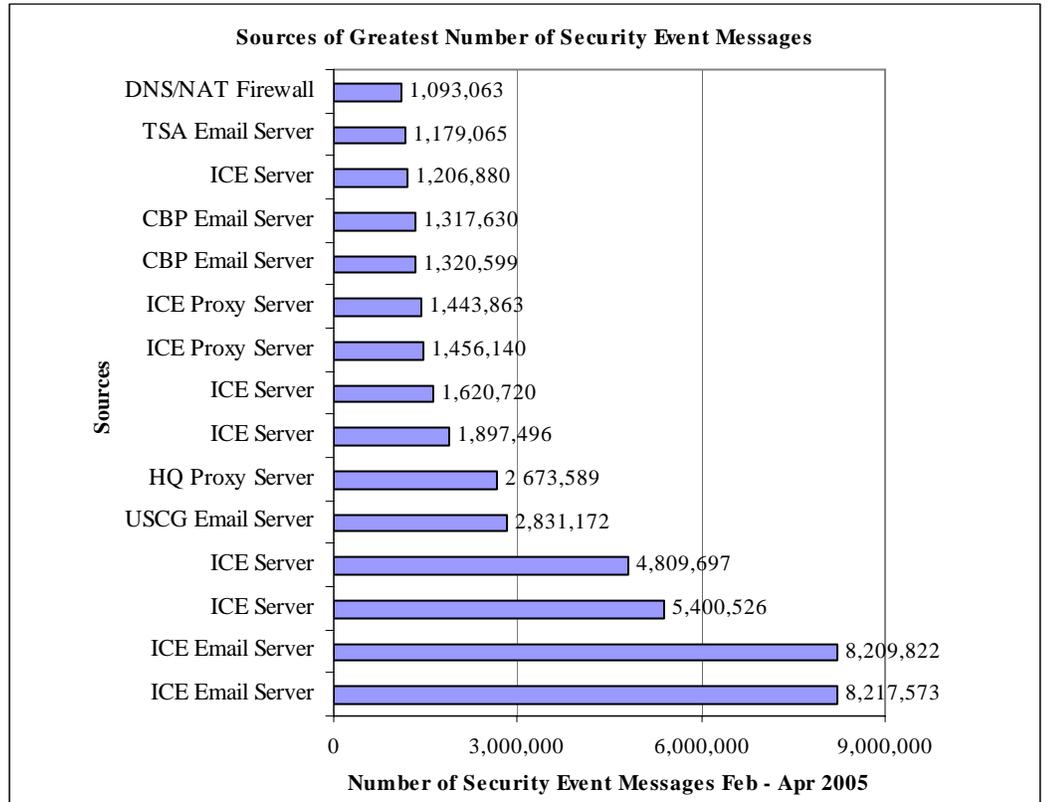


Definitions for the “Top Ten Security Event Messages”:

1. ids.detect.suspicious – these events usually encompass tags and alerts of a suspicious nature, for example SMB:NAME-WILDCARD and SMB:IPC-ATTEMPT. They are very common on a mostly Microsoft network.
2. ids.detect.recon.icmp - these events are alerts and tags reported as ICMP:L3-RETRIEVER and ICMP:SUPERSCAN. In a mostly Microsoft network, they are very common.
3. ids.detect.misuse.porn – these events are found in the case of porn tags or alerts. These events have a high likelihood of being a “false positive”. For example, intrusion detection system sensors are looking for a known string, for example “oral”. However this string might be present within other legitimate words such as “behavioral.”

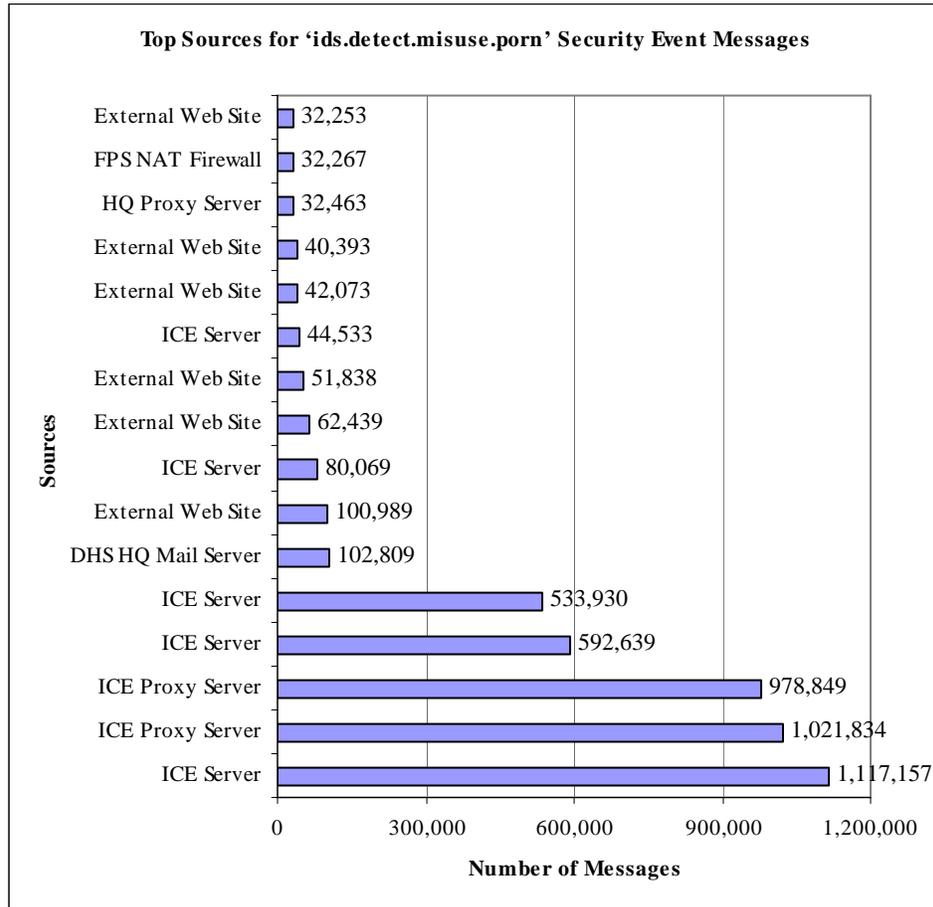
4. ids.detect.suspicious.proxy - this type of event covers tags and alerts of a suspicious nature as applies to proxy servers, such as PROXY:WEB-GET and PROXY:WEB-POST in dragon. There is a lot of 'getting' and 'posting' on internal websites with-in DHS, which can cause this event.
5. ids.detect.recon.snmp - this type covers reconnaissance activity using the simple network management protocol (SNMP), a set of protocols for managing complex networks. Most of these are probes such as SNMP:PUBLIC.
6. ids.detect.failure.mail – these events are tags or alerts reported when email fails to deliver. It is common from Microsoft Exchange Servers (i.e.: Microsoft Outlook Exchange).
7. ids.detect.unknown.dragon - this type covers tags/alerts that are not known, a “miscellaneous” category.
8. ids.detect.recon.udp – this type of event, tags and alerts reported as UDP-SWEEP, is another reconnaissance activity which uses the User Datagram Protocol (UDP). The ICE and DHS wide area networks generate many of these messages.
9. ids.detect.exploit.os - this type of event occurs with activity that might be associated with the exploitation of vulnerability. Like the PORN alerts, the intrusion detection system is looking for strings like “DATE” and “UNAME.” Server-to-server communications also generate these events that are commonly determined to be false positives.
10. ids.detect.suspicious.web - this type of event covers activity that is considered suspicious web traffic. This can often involve a suspicious file name or command being detected, such as a typical file name for an executable file/application. It is important to remember, that the intrusion detection system is looking for the string and does not distinguish between plain text and an actual executable file.

Appendix D
 Top Sources for Most Security Event Messages



Note: We obtained security event messages for February, March, and April 2005. We determined which devices or sites were the greatest sources of security event messages in one of those three months. Then we combined the number of security event messages for each of those three months. We then identified those IP addresses that produced more than one million security event messages to produce this chart.

Appendix E
Top Sources for 'ids.detect.misuse.porn' Security Event Messages



Note: We obtained security event messages for February, March, and April 2005. We determined which devices - or sites - were the greatest sources of 'ids.detect.misuse.porn' security event messages in one of those three months. Then we combined the number of security event messages for each of those three months to produce this chart.

October 2004:

The Deputy Secretary requested specific documentation before the ITP entered the Capability Development and Demonstration Phase.

January 18, 2005:

ITP program documentation was provided to the IRB.

March 11, 2005:

The Under Secretary for Management said that the ITP was not ready for IRB review.

March 17, 2005:

The DHS Chief Financial Officer (CFO) noted that the ITP implementation was beyond the authority granted. The CFO asked that the program submit a Management Review Council (MRC) request for approval pending an IRB review.

April 12, 2005:

The DHS OneNetwork was granted an “Interim Approval to Operate” for six months by the DHS CIO.

April 18, 2005:

The Director of the ITP submitted a request for approval to proceed with implementation of the ITP, including the OneNetwork component.

April 20, 2005:

The acting Deputy CIO directed a 45-day assessment of the ITP be performed.

May 18, 2005:

Phase 1 of the OneNetwork implementation completed.

Information Systems and Architectures Division

Roger Dressler, Director
Kevin Burke, Audit Manager
Karen Nelson, Audit Team Lead
Domingo Alvarez, Auditor
Danielle Zook, Program Analyst
William Matthews, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretariat
Assistant Secretary for Policy
Under Secretary, Management
DHS Audit Liaison
Chief Information Security Officer
Assistant Secretary, Public Affairs
CIO Audit Liaison
Director, Compliance and Oversight Program, OCIO
Assistant Secretary, Legislative Affairs

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

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or, email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.