Department of Homeland Security
Office of Inspector General

Better Monitoring and Enhanced Technical Controls Are Needed to Effectively Manage LAN-A

(Redacted)

OIG-09-55

April 2009

Office of Inspector General

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

Homeland Security

April 10, 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 headquarters network, known as LAN-A. It is based on interviews with selected officials and contractor personnel, direct observations, technical scans, 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
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

ATO	Authority to operate
CO	Contracting Officers
CONOPS	Concept of Operations
COTR	Contracting Officer Technical Representatives
DAA	Designated Accreditation Authority or Designated Approving Authority
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
FY	Fiscal Year
IT	Information Technology
ITAC	Information Technology Acquisitions Center
ITMS	Information Technology Management Services
IT-NOVA	Information Technology Network Operations Virtual Alliance
ITSO	Information Technology Services Office
NIST	National Institute of Standards and Technology
O&M	Operations and Maintenance

Table of Contents/Abbreviations

OCIO	Office of Chief Information Officer
OCPO	Office of Chief Procurement Officer
PAR	Privilege Account Request
POA&Ms	Plan of Action and Milestones
PRISM	Purchase Request Information System
SLA	Service Level Agreements

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

LAN-A is the Department of Homeland Security (DHS) unclassified headquarters' network. The network provides email and data communication services for all headquarters personnel in the Washington, DC, metropolitan area. In mid 2007, DHS consolidated services from several information technology (IT) related contracts into the Information Technology Network Operations Virtual Alliance (IT-NOVA) to help it manage LAN-A more effectively.

We evaluated network operations to determine whether DHS is effectively managing LAN-A. In addressing our objective, we determined whether the contractor has provided adequate support services in accordance with the contract terms; effective system controls have been implemented to protect the network; and program officials have ensured that LAN-A was certified and accredited in accordance with DHS information security policy.

Overall, DHS has implemented effective system controls to protect the information stored and processed by the system. For example, DHS ensures that patch management and vulnerability assessments are performed periodically on LAN-A. In assessing the controls that have been implemented, we identified only a few missing security patches. In addition, audit trails were enabled on servers, workstations, and routers. Finally, the IT-NOVA Operations and Maintenance (O&M) contractor has established an IT Service Desk to provide 24 hour end users support.

However, additional monitoring of the contract is needed to ensure that the contractor is providing adequate services and the required deliverables. In addition, DHS can make improvements in managing its privileged and applying security patches, Finally, DHS must ensure that LAN-A is reaccredited according to applicable guidance, and that the required security documents are developed and continuously updated.

We are making 10 recommendations to the Under Secretary for Management and Chief Information Officer. The department concurred with our recommendations and has already begun to take actions to implement them. The department's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

LAN-A, DHS' unclassified network, provides email and data communication services for all headquarters personnel in the Washington, DC, metropolitan area. The IT Services Office (ITSO) within the Office of the Chief Information Officer (OCIO) is responsible for maintaining the network. Most LAN-A users are from headquarters components and offices, such as Domestic Nuclear Detection, Management, National Protection and Programs, and Science and Technology.

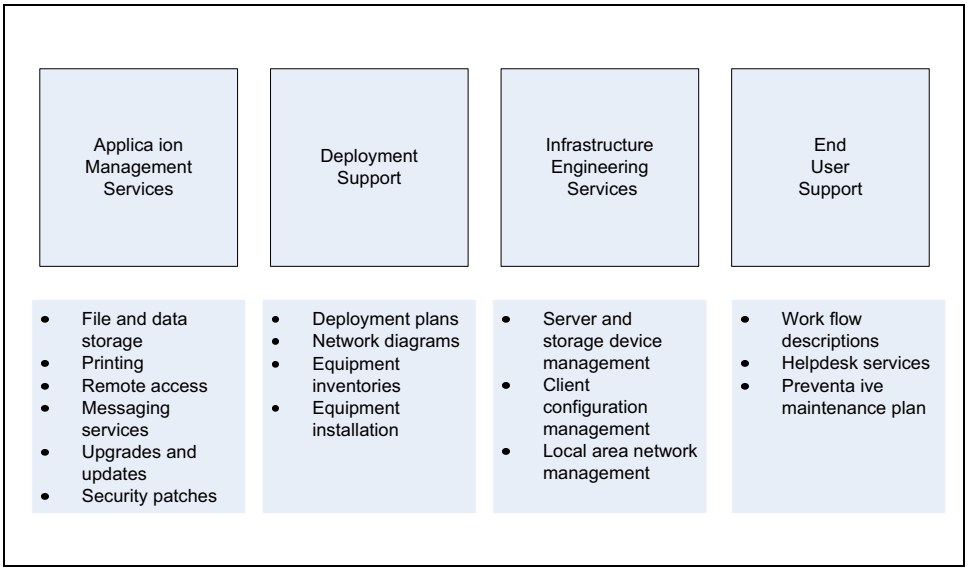
In June 2006, LAN-A was compromised when malicious software was installed on 150 of DHS' workstations.[1] Subsequent reviews, including a congressional investigation, revealed that the LAN-A contractor had not fulfilled its responsibilities to install security devices or elevate security incidents to DHS officials. Specifically, investigators found that the contractor had installed only three of the required seven intrusion detection devices at the time of the compromise.

Following this incident, in mid-2007, the department consolidated services from several IT-related contracts into IT-NOVA. DHS awarded two task orders under IT-NOVA: was awarded an O&M task order and was awarded a Project Management Office task order. During this audit, we focused on reviewing the IT services and contractor performance provided under the IT-NOVA O&M task order.

The IT-NOVA O&M task order included a full range of IT support services. A list of task order components and services is shown in Figure 1. Specifically, was tasked with providing support for all network services, including user support and security monitoring.

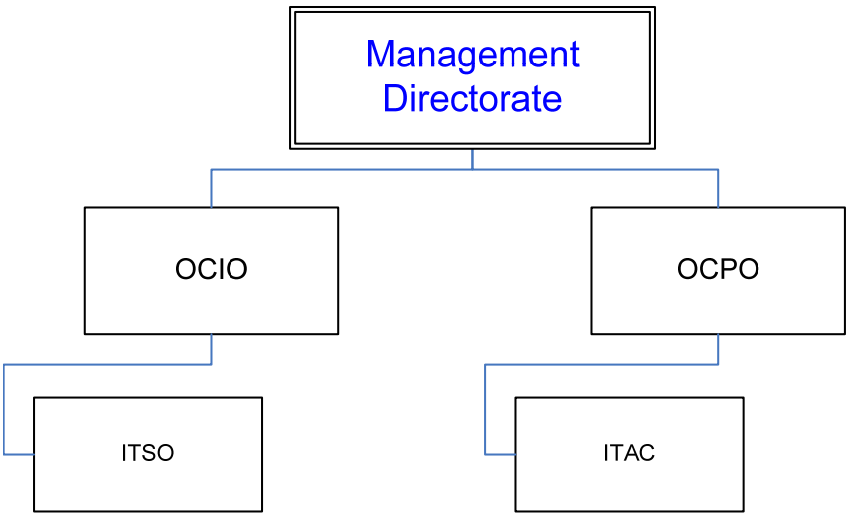
[1] Malicious software is a general term for programs that, when executed, cause undesired results on a system. The malicious software used in this attack sent unclassified data from DHS' systems to Chinese language websites.

Figure 1: IT-NOVA O&M Task Order Support Services



The IT-NOVA task order is managed by two offices within the Management Directorate. The technical oversight of the task order is provided by the ITSO. Contracting and procurement oversight for IT-NOVA are provided by staff from the Office of Chief Procurement Officer (OCPO) IT Acquisitions Center (ITAC). Figure 2 outlines the IT-NOVA management structure, including the OCIO, ITSO, OCPO, and ITAC.

Figure 2: IT-NOVA Management Structure



Results of Audit

OCIO Has Taken Initial Steps to Improve LAN-A Management

OCIO has taken some positive steps to improve LAN-A management and security. For example, patch management and vulnerability assessments are being performed periodically on LAN-A. These actions help to identify and mitigate network security vulnerabilities. During our security testing, security patches were being applied. In addition, audit trails recording user login activities were enabled on servers, workstations, and routers.

Furthermore, the O&M contractor has established an IT Service Desk to provide 24 hour user support for applications and network services. The IT Service Desk has maintained customer service satisfaction levels above 90% for August, September, and October 2008.

These actions have improved the security and reliability of LAN-A. Yet, DHS can make further improvements to effectively manage the network. For example, additional monitoring of contractor performance is needed to effectively administer the IT-NOVA task order. In addition, DHS needs to ensure that detailed procedures for IT and security related activities are documented. Furthermore, improvements can be made in technical controls to strengthen the network's information security. Finally, DHS must ensure that security documents are updated prior to re-certifying and accrediting LAN-A.

Additional Monitoring Is Needed to Administer LAN-A IT Contract Services

OCIO is not effectively administering the O&M contract requirements. For example, OCIO has not provided clear guidance and exercised sufficient oversight necessary to ensure that the contractor has delivered the full range of IT services and related documentation required by the contract. Furthermore, OCIO has not taken the actions needed to address and correct deficiencies identified in the contractor's performance. As a result, certain contract service requirements have not been met.

O&M Contract Administration Issues

OCIO has not defined its responsibilities for LAN-A program management oversight, including communication with the contractor to ensure that the contractor provides adequate IT support to users. In addition, OCIO has faced challenges coordinating the work of various contractors within ITSO. This has led to contractor delays in troubleshooting LAN-A problems related to its network and applications, and in responding to user requests.

Furthermore, OCIO has not ensured that the contractor receives tasking direction only from authorized contracting officials. We identified instances where senior program officials, who have not been given contractual authority, have instructed contractor personnel to perform services that are not in accordance with the terms stated in the task order.

The need for additional staff at OCIO has contributed to the insufficient coordination between various contractor efforts or responding to users' issues timely. Specifically, the Director of the Headquarters Services division estimated that the division requires twice as many staff members to manage the size and scope of services under the IT-NOVA task order. Due to inadequate monitoring and oversight, there have also been delays in authorizing task order payments and providing technical support services that had not been authorized by the proper personnel.

OCIO Has Not Provided Clear Guidance and Defined Reporting Requirements

OCIO has not provided guidance to the contractor regarding the content and details that should be included in the contractor's monthly LAN-A performance and quality control reports. As a result, the contractor has not been providing these monthly reports. Without these reports, OCIO does not have the necessary information to evaluate contractor performance.

Beginning in June 2008, the IT-NOVA O&M task order required that the contractor provide monthly performance summary reports containing information on the dates, times, and duration of outages or service interruptions on DHS applications, network environments, and databases. In addition to the monthly performance reports, the contractor agreed to provide the department with a monthly quality control plan. The quality

control plan describes how the contractor will control the equipment, systems, or services in order to meet the task order requirements. The plan would then be used as the basis for the monthly quality control reports. OCIO did not immediately approve the quality control plan that was submitted in May 2008. Furthermore, since OCIO had not provided clear guidance on the content to be included in the monthly reports, at the request of OCPO, the contractor suspended providing this information to the department.

In December 2008, we informed OCIO that the department was not receiving the information needed to properly evaluate and monitor contract performance as it relates to LAN-A. Subsequent to that meeting, a procurement official informed us that the quality control plan was approved by OCIO. Additionally, both OCIO and the contractor agreed on the content for the monthly reports. The contractor is to begin submitting future monthly performance summary and quality control reports starting in January 2009.

OCIO Has Not Responded to LAN-A Contractor Performance Deficiencies

OCIO has not timely responded to contractor deficiencies identified. Specifically, OCIO officials have not ensured that the deficiencies identified in contractor service support are being addressed.

On April 17, 2008, the contracting officer issued a quality discrepancy report,[2] which outlined issues regarding the performance of the O&M contractor. The quality discrepancy report identified that the contractor had not met all service requirements for the IT Service Desk and had not appointed the necessary senior staff to the engineering, operations, and applications areas. This formal report required the contractor to address the identified deficiencies and respond with a proposed corrective action plan within 10 days.

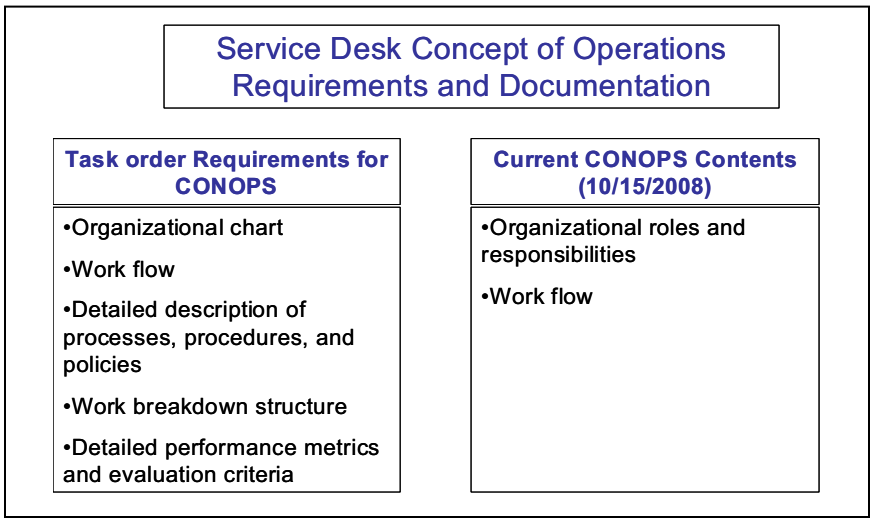
On May 1, 2008, the contractor responded with an action plan and requested a meeting with OCIO to discuss its response. On June 11, 2008, the contracting officer tasked OCIO staff, including the contracting officer technical representative, to review and respond to the contractor's action plan by June 16, 2008. OCIO,

[2] A quality discrepancy report is a formal notification from the contracting officer to the contractor regarding contractual performance. The report allows the contractor an opportunity to correct or replace nonconforming services or supplies.

however, never responded to the contractor's action plan. In a follow-up meeting on June 19, 2008, the contracting officer decided to close the performance deficiencies identified without further recourse.

In addition to the deficiencies noted in the quality deficiency report, we determined that the contractor has not documented the processes and procedures for IT and information security activities. For example, the contractor was required to develop a comprehensive concept of operations (CONOPS) with documented processes and procedures for the IT Service Desk. We determined that the CONOPS developed has not met all the requirements, as noted in Figure 3.

Figure 3: IT Service Desk Operations



Due to staffing shortages, OCIO has not been able to adequately monitor the O&M contractor requirements, perform its program management oversight functions or properly evaluate contractor performance. As of September 2008, ITSO had staffed only 60% of its available federal positions. OCIO officials recognize that staffing shortages for federal positions remain an issue for ITSO. Further, we reported that DHS faced significant challenges in establishing an effective IT management structure to oversee IT resources.[3] Without sufficient monitoring, oversight, and staffing, there is little assurance that the O&M service support provided for LAN-A is adequate.

[3] *Progress Made in Strengthening DHS Information Technology Management, But Challenges Remain*, dated September 2008 (OIG-08-91).

Recommendations

We recommend that the Under Secretary for Management direct the Chief Information Officer to:

Recommendation #1: Strengthen the department's monitoring oversight of the O&M contractor to ensure that services are provided in accordance with the task order.

Recommendation #2: Obtain required monthly reports and the IT Service Desk procedures from the O&M contractor.

Recommendation #3: Take steps to ensure that only personnel with appropriate contractual responsibility can provide direction to the contractor to perform its tasks; and provide clear and sufficient guidance to the contractor to perform its services.

Recommendation #4: Address the deficiencies identified in the contractor's performance.

Management Comments and OIG Analysis

DHS concurred with recommendation 1. DHS agreed that the department must strengthen its oversight of the O&M contractor and ensure contractual obligations are adequately met. DHS has developed Service Level Agreements (SLAs) for contractor performance, and updated the department's current practices to monitor and evaluate contractor performance. DHS will negotiate with the contractor to add SLAs and enhanced service metrics, aimed at tracking and improving the contractor's performance. DHS anticipates completing the negotiations and having the SLAs added to the contract by the third quarter of FY 2009.

We agree that the steps DHS are taking, and plans to take, begin to satisfy this recommendation.

DHS concurred with recommendation 2. DHS agreed that the required monthly deliverables must be consistently submitted, reviewed, and approved by government staff. The department acknowledged that this requirement has not been occurring on a consistent basis. Furthermore, DHS agreed that when the contractor is unable to provide a required deliverable, it must be documented in a performance deficiency letter and followed up with to ensure swift resolution. The contractor has drafted a

CONOPS for the IT service desk. DHS will complete its review within 30 days of their response to either accept or reject these standard operating procedures. Finally, OCIO will make monthly on-site monitoring visits to ensure daily and weekly monitoring and reporting for effectiveness and to solicit feedback from the stakeholder for contractor performance.

We agree that the steps DHS are taking, and plans to take, begin to satisfy this recommendation.

DHS concurred with recommendation 3. DHS agreed that the department must adhere to the Federal Acquisition Regulation to ensure that only Contracting Officers (CO) and Contracting Officer Technical Representatives (COTR) provide direction to contractor personnel to perform its tasks. Immediately, DHS will strengthen its oversight to ensure that only authorized government personnel with contractual responsibilities, i.e., CO, COTR, can provide direction to contractor personnel. DHS will review all deliverables to monitor the process and ensure contractor compliance. In addition, the department will ensure that only authorized personnel, i.e., CO, COTR, can commit DHS to any type of contractual obligation and only to the extent of their delegated authority. Personnel responsible for contracts shall maintain a close and continuous relationship with the CO to ensure that acquisition personnel are made aware of contemplated acquisition actions. DHS believes that these changes will improve the department's planning for acquisition action and provide more timely, efficient economical acquisition, and contractor oversight. Finally, DHS acknowledged that personnel who are not delegated contracting authority or insufficient contracting authority shall not commit the Government, formally or informally, to any type of contractual obligation. All OCIO personnel were scheduled to receive a briefing on the responsibility of government contractual personnel by February 19, 2009.

We agree that the steps DHS are taking, and plans to take, begin to satisfy this recommendation.

DHS concurred with recommendation 4. DHS agreed that the department must follow-up on the deficiencies identified throughout contractor performance in a timely and thorough manner. To improve the quality and efficiency of the department's monitoring process, DHS will conduct monthly reviews with the contractor's senior management and document deficiencies for future actions.

We agree that the steps DHS are taking, and plans to take, begin to satisfy this recommendation.

Enhancements Can Be Made in LAN-A Technical Controls

OCIO does not have an effective process to manage its LAN-A privileged accounts or ensure that security patches are deployed on applications. For example, OCIO has not defined the system administrators' responsibilities for deploying security patches. As a result, there is greater risk that security controls implemented to protect LAN-A may be circumvented.

Privileged Accounts Are Not Properly Managed and Maintained

OCIO does not have an effective process to manage its LAN-A privileged accounts to ensure that only those authorized to perform administration duties have the appropriate permissions. Privileged accounts are those having elevated access permissions only granted to system administrators to perform their network related job functions. When the privileged accounts are not properly managed, it may allow malicious users the capability to bypass security features and have unmonitored access to system configuration settings and data.

To request elevated access permissions, users are required to complete an access request form. The form is then routed to appropriate personnel for review and approval. Once the request has been approved, users are assigned to the groups to perform their network related functions.

While OCIO has established a process for requesting and granting elevated access permissions, this process has not been fully implemented. For example:

- As of November 2008, accounts have been granted to contractors who manage LAN-A
- A domain administrator was granted enterprise administrator access This assignment of permissions, done without documented management approval, circumvents the access permission request process and Since no documented approval and audit trails were available, we could not determine who modified the group policy to grant domain administrator higher access permission.

-
-

- [redacted]

Elevated account access, such as that granted to system administrators, must be managed properly to prevent unauthorized access to LAN-A. Poor management and maintenance of privileged accounts may increase the risks of individuals exploiting these accounts to gain unauthorized access to the network and DHS assets.

[redacted]

[redacted] Further, while audit trails are enabled on routers, servers, and workstations, [redacted]

[redacted]

[redacted]

Documented LAN-A Patch Management Process Has Not Been Established

While security patches were applied to servers and workstations, DHS does not have documentation outlining specific duties, roles, and responsibilities regarding the LAN-A patch management program. Documented procedures can ensure that security patches are deployed in a consistent manner.

on a monthly basis. Security patches are tested and evaluated before they are deployed to verify that security patches have been deployed.

To evaluate the patch management process for LAN-A, we interviewed administrator personnel, examined documentation, and performed vulnerability testing on a sample of servers, workstations, and network devices. Of the 453 LAN-A devices that were tested, we identified the following high-risk vulnerabilities that may be exploited if they are not properly mitigated:

-
-
-
-
-

DHS requires that security patches be installed in a timely and expeditious manner. The National Institute of Standards and Technology (NIST) also recommends that agencies have an explicit and documented patching and vulnerability policy as well as a systematic, accountable, and documented set of processes and procedures for handling patches. Documented procedures should specify the techniques an agency will use to monitor for new patches and vulnerabilities and the personnel responsible for such monitoring.

Without a documented patch management process to support the security program for LAN-A, DHS cannot ensure that all vulnerabilities have been mitigated to prevent malicious users from gaining uncontrolled access to LAN-A. Applying security patches is critical for securing LAN-A and protecting sensitive data from unauthorized access, manipulation, and misuse.

Inadequate management of privileged accounts, weaknesses identified in patch management, and

These weaknesses may allow malicious users to bypass or disable computer access controls and undertake a wide variety of inappropriate or malicious acts.

Recommendations

We recommend that the Under Secretary for Management, direct the Chief Information Officer to:

Recommendation #5: Establish a process to ensure that LAN-A

Recommendation #6: Ensure that the authorization for privileged LAN-A access is documented, reviewed and approved by appropriate officials.

Recommendation #7: Develop a documented process to deploy security patches on LAN-A.

Recommendation #8:

Management Comments and OIG Analysis

DHS concurred with recommendation 5. DHS noted that the policies that govern privileged accounts need to be stricter than those of regular user accounts. In addition, DHS

We agree that the steps DHS are taking, and plans to take, begin to satisfy this recommendation.

DHS concurred with recommendation 6. DHS noted that the department has established a process to ensure that the requests for privileged LAN-A accounts are documented, reviewed, and approved by appropriate officials. DHS also acknowledged that more resources must be dedicated to auditing this process. Currently, all request/business justifications for privileged accounts must be submitted to the helpdesk via a Privileged Account Request (PAR) through the requestor's immediate supervisor, approved by the government lead of Operations, and then approved by the LAN-A Security Manager. Beginning in the third quarter of FY 2009, DHS will perform a bi-monthly audit of privileged accounts to ensure that no accounts were created outside of this process. In addition, DHS will establish a one year expiration date for all PARs and will require customers to re-apply through the approval process if the requirement for said account still exists.

We agree that the steps DHS are taking, and plans to take, begin to satisfy this recommendation.

DHS concurred with recommendation 7. DHS noted that a draft copy of the standard operating procedures for deploying security patches on LAN-A was provided to the OIG during the audit. In order to have an effective patch management process, DHS acknowledged that the draft procedures require revision to include branch manager approval, and consistent execution. Finally, DHS maintained that security patches are being applied on LAN-A as only a few missing security patches were identified during the audit.

We agree that the steps DHS are taking, and plans to take, begin to satisfy this recommendation.

DHS concurred with recommendation 8.

We agree that the steps DHS are taking, and plans to take, begin to satisfy this recommendation.

Compliance with DHS Information Security Program

LAN-A program officials do not ensure that security documents required by the department, e.g. system security plan, plan of action and milestones (POA&Ms), etc, are periodically updated and contain the necessary information for the DAA to make a credible decision to re-certify and accredit LAN-A.[4] DHS and NIST require that security documents be included as part of the accreditation package and be updated periodically.

According to NIST guidance, the certification & accreditation process, when applied to agency information systems, provides a systematic approach to assess whether the management, operational, and technical security controls are effectively implemented. Status reporting and periodic update of security documentation is one of the tasks that must be performed during the continuous monitoring phase. The purpose of status reporting and maintaining security documentation current is to: (1) update the system security plan to reflect the proposed or actual changes to the information system; (2) update the POA&Ms based on the activities carried out during the continuous monitoring phase; and (3) report the security status of the information system to the authorizing official and senior agency information security officer.

[4] According to applicable NIST guidance, continuous monitoring of security controls and updating system documentation is a critical aspect of the certification & accreditation process in the post-accreditation period. The purpose of this phase is to provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the authorizing official when changes occur that may impact the security of the system. Continuous monitoring results should be documented and reported to the authorizing official on a regular basis. The monitoring results should also be considered when making updates to the system security plan and to the POA&Ms because the authorizing official and the certification agent will use these security documents to make the accreditation decision.

The activities in this phase are performed continuously throughout the life cycle of the information system.

After the original accreditation expired in July 2008, the DAA granted an authority to operate (ATO) of six months to LAN-A. However, even though the DAA was not given the most updated and credible information to reaccredit the network, LAN-A was reaccredited anyway. For example, the system security plan has not been updated since LAN-A was accredited in July 2005. For FISMA reporting purposes, the Chief Information Officer reviews accreditation packages for all information systems for compliance with applicable DHS and NIST guidance. After reviewing the accreditation package for LAN-A, the Chief Information Officer did not accept the accrediting official's ATO because the network was reaccredited without the required security documents. In its Fiscal Year 2008 FISMA submission to the Office of Management and Budget, the Chief Information Officer reported that LAN-A was one of the systems without an ATO.

In a November 2008 meeting, a program official indicated that DHS was in the process of defining a new system boundary for LAN-A and reaccrediting the network. According to the program official, the required security documents are being developed in accordance with applicable DHS and NIST guidance.

DHS requires security documents to be part of the accreditation package and be updated periodically. Specifically, DHS requires the following 11 documents to support the accreditation decision: ATO letter, system security plan, security assessment report, risk assessment, security test and evaluation, contingency plan, contingency plan test results, Federal Information Processing Standard 199 determination, e-authentication determination, privacy threshold analysis, and NIST Special Publication 800-53 assessment.

Understanding the overall effectiveness of security controls for an information system is essential in determining the risk to DHS' operations and assets. Without the updated security documents, program officials cannot make credible risk-based decisions on whether to authorize systems to operate or ensure that systems are adequately secure.

Recommendations

We recommend that the Chief Information Officer direct the LAN-A Information Systems Security Manager to:

Recommendation #9: Develop all required security documents according to applicable DHS and NIST guidance before LAN-A is reaccredited.

Recommendation #10: Maintain and update periodically security documents that support LAN-A's accreditation.

Management Comments and OIG Analysis

DHS concurred with recommendation 9. LAN-A program officials acknowledge the need and intent to verify that all appropriate and applicable security documents are completed for LAN-A's re-accreditation. However, the program officials believed that the network was accredited in accordance with NIST standards. After a security assessment was performed in July 2008, program officials maintained that the DAA had a reasonable measure of risk and decided to accredit LAN-A for a short period of time. The program officials added that LAN-A's accreditation was consistent with NIST guidance which allows the DAA to make a reasonable assumption of risk based on the information presented to support the decision.

Without the required security documents, we maintain that LAN-A's July 2008 accreditation was not consistent with applicable DHS and NIST guidance. In particular, NIST requires that the system security plan be provided to the DAA, as part of the accreditation package, along with the results from the security assessment to make a credible, risk-based decision on whether to accredit the system. The system security plan can also contain, as supporting appendices or references to other key security documents, such as the risk assessment, privacy impact assessment, contingency plan, incident response plan, configuration management plan, security configuration checklists, and any system interconnection agreements. At the time LAN A was accredited in July 2008, all security documents were outdated. As a result, the DAA did not have the necessary information to make a credible decision to certify and accredit the LAN A.

DHS concurred with recommendation 10. DHS has divided the network into four manageable general support systems and will

ensure each is fully documented. Accreditation packages will be developed for each system, and maintained and updated periodically.

We agree that the steps DHS are taking, and plans to take, begin to satisfy this recommendation.

Appendix A
Purpose, Scope, and Methodology

The objective of this review was to determine whether DHS is effectively managing its headquarters' local area network, known as LAN-A. Specifically, we determined whether: (1) the contractor provided adequate support services according to the contract terms; (2) effective controls have been implemented to protect the network; and (3) FISMA requirements have been implemented.

We interviewed selected personnel at DHS headquarters; data centers located at Clarksville, Virginia, and Stennis Space Center, Mississippi; and IT-NOVA Service Desk Operations at Indianapolis, Indiana. In addition, we reviewed and evaluated DHS security policies and procedures, the IT-NOVA task order, and other appropriate documentation. During the audit, we used software tools, such as NESSUS and NMAP to detect, analyze, and evaluate the effectiveness of controls implemented on selected servers, workstations, and switches. Upon completion of the assessments, we provided program officials with the technical reports detailing the specific vulnerabilities detected on LAN-A network devices and the actions needed for remediation

We conducted this audit between July and December 2008 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 C.

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

MAR 20 2009

MEMORANDUM FOR: Richard L. Skinner
Inspector General

FROM: Elaine C. Duke
Under Secretary for Management

SUBJECT: Response to OIG Draft Report, "Better Monitoring and Enhanced Technical Controls are Needed to Effectively Manage LAN A"

The Department of Homeland Security (DHS) Office of the Chief Information Officer (OCIO) has initiated efforts to address the findings of the Office of the Inspector General Draft Report, *Better Monitoring and Enhanced Technical Controls are Needed to Effectively Manage LAN A*, dated January 23, 2009. The response is as follows:

Recommendation #1- Strengthen the Departments monitoring oversight of the O&M contractor to ensure that services are provided in accordance with the task order.

OCIO agrees that it must strengthen its oversight of the Operations and Management (O&M) contractor and ensure contractual obligations are adequately met. We have developed Service Level Agreements (SLAs) for contractor performance and have updated our current practices to monitor and evaluate contractor performance. We will negotiate with the contractor to add SLAs and enhanced service metrics aimed at tracking and improving user performance to the contract. We anticipate completing negotiations and having SLAs on contract by third quarter Fiscal Year (FY) 2009.

Recommendation #2- Obtain required monthly reports and the IT Service Desk procedures from the O&M contractor.

OCIO agrees that required monthly deliverables must be consistently submitted, reviewed and approved by government staff and that this has not been occurring on a consistent basis. A contractor's inability to provide said deliverable must be documented in performance deficiency letters and followed up with to ensure swift resolution. A Concept of Operations for the IT Service Desk has been drafted by the contractor. The government will complete its review within the next 30 days and either accept or reject this Standard Operating Procedure (SOP). OCIO will make monthly on-site monitoring visits to ensure daily and weekly monitoring and reporting for effectiveness and to solicit feedback from the stakeholder for contractor performance.

Recommendation #3- Take steps to ensure that only personnel with appropriate contractual responsibility can provide direction to the contractor to perform its tasks; and provide clear and sufficient guidance to the contractor to perform its services.

OCIO agrees that it must better adhere to the Federal Acquisition Regulation and ensure that only Contracting Officers and Contracting Technical Representatives (COTR) provide direction to the contractor support to perform its tasks. OCIO will immediately provide better oversight and ensure that no government representative provides unauthorized direction to contract support. OCIO will review all reports for monitoring process to provide full time oversight for contractor compliance.

In addition, only authorized OCIO COTR personnel shall commit OCIO to any type of contractual obligation and only to the extent of their delegated authority. Personnel responsible for contracts shall maintain a close and continuous relationship with the contracting officer to ensure that acquisition personnel are made aware of contemplated acquisition actions. This will be mutually beneficial in terms of better planning for acquisition action and more timely, efficient and economical acquisition and contractor oversight. Personnel not delegated contracting authority or insufficient contracting authority shall not commit the Government, formally or informally, to any type of contractual obligation. All OCIO personnel was briefed on February 19, 2009 on the responsibility of government personnel contractual responsibility.

Recommendation #4- Address the deficiencies identified in the contractors performance.

OCIO agrees that it must follow through on deficiencies identified throughout contract performance notifications in a timely and complete manner. OCIO will monitor process management to increase the quality and efficiency by conducting monthly reviews with contractor's senior management and document deficiencies for future actions.

Recommendation #5- [redacted]

The policies that govern a privileged account need to be stricter than those of a regular user account, not the contrary. OCIO agrees that the process by which [redacted]

Recommendation #6- Ensure that the authorization for privileged LAN-A access is documented, reviewed and approved by appropriate officials.

OCIO agrees and we have a process by which privileged LAN-A account requests are documented, reviewed and approved by appropriate officials, but we acknowledge that more

resources must be dedicated to auditing this process. Currently, all requests/business justifications for privileged accounts must be submitted to the helpdesk via a Privileged Account Request (PAR) through the requestor's immediate supervisor, approved by the government lead of Operations and then approved by the Security Manager of LAN-A. A requestor's electronic submission of this form implies acknowledgement of the Rules of Behavior that accompanies each request. As noted in our response to recommendation #5, in third quarter of FY09 OCIO will begin a bi-monthly audit of Privileged Accounts to make sure that no accounts were created outside of this process. OCIO will also set an expiration of one year on all PAR requests and will require customers to re-apply through the approval process if the requirement for said account still exists.

Recommendation #7- Develop a documented process to deploy security patches on LAN-A.

OCIO agrees; however, we would like it noted that this recommendation refers to a SOP document that was provided to the IG in draft form upon inspection. The recommendation is misleading and implies that security/system patching is not occurring on LAN-A which is contrary to what the IG observed throughout inspection. OCIO acknowledges that this draft document requires revision to include branch manager approved hand-offs and consistent execution to be successful.

Recommendation #8- [redacted]

[redacted]

Recommendation #9- Develop all security documents according to applicable DHS and NIST guidance before LAN-A is re-accredited and Recommendation #10- Maintain and update periodically security documents that support LAN-A's accreditation.

OCIO agrees and would like it noted that at the time of the IG inspection, LAN-A was recognized as accredited by the National Institute Standards Technology (NIST) Standards. NIST standards state that so long as the Designated Approving Authority can make a reasonable determination of risk (NIST *guidelines* refer to artifacts that support this determination), then a reasonable assumption of risk can be made. In July of 2008, following a thorough National Security Agency Blue Team Assessment, the Designated Accreditation Authority had a reasonable measure of risk and consequently accepted said risk for a very short duration.

OCIO acknowledges and intends to verify that all appropriate and applicable documents are completed for LAN-A's re-accreditation and will maintain this package through Continuous

Monitoring throughout its lifecycle. The Chief Information Security Office of DHS HQ has broken LAN-A out into four manageable General Support Systems (GSS) and will assure each has been fully documented:

- LAN-A Core Services (Active Directory, File/Print)
- LAN-A Management Zone (Anti-virus, Windows Update, Vulnerability Management, etc) **COMPLETED**
- LAN-A Exchange Infrastructure (Exchange, Outlook Web Access, Blackberry, E-vault)
- LAN-A User Enclaves and Network Infrastructure

Appendix C
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
Charles Twitty, IT Auditor
Kristina Hayden, Program Analyst
Amanda Strickler, IT Specialist
Nazia Khan, IT Specialist
Thomas Rohrback, IT Specialist
David Bunning, IT Assistant

Karen Nelson, Referencer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Acting Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Acting General Counsel
Executive Secretariat
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
Chief Information Officer 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) 254-4199, 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.