



Department of Homeland Security Office of Inspector General

Stronger Security Controls Needed on Active Directory Systems



Office of Inspector General

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



**Homeland
Security**

MAY 10 2010

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 implementation of Active Directory. It is based on interviews with selected officials and contractor personnel, direct observations, technical security vulnerability assessments, and a review of applicable documents.

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

Richard L. Skinner
Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Executive Summary	1
Background	2
Results of Audit	3
Vulnerable Systems Added to DHS Network.....	3
Governance Needed to Verify Security Requirements	5
Recommendations.....	6
Management Comments and OIG Analysis	6

Appendixes

Appendix A: Purpose, Scope, and Methodology.....	8
Appendix B: Management Comments to the Draft Report	9
Appendix C: Major Contributors to This Report.....	14
Appendix D: Report Distribution.....	15

Abbreviations

CBP	Customs and Border Protection
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
HQ	Headquarters
ICE	Immigration and Customs Enforcement
ISA	Interconnection Security Agreement
OCIO	Office of Chief Information Officer
OCS	Office Communication Server
OIG	Office of Inspector General
S&T	Science and Technology (Directorate)
TSA	Transportation Security Administration
USCIS	United States Citizenship and Immigration Services
USCG	United States Coast Guard
USSS	United States Secret Service



Department of Homeland Security
Office of Inspector General

Executive Summary

The Department of Homeland Security uses Microsoft Windows Active Directory services to manage users, groups of users, computer systems, and services on its headquarters network. We reviewed the security of the Active Directory collection of resources and services used by components across the department through trusted connections. These resources and services provide department-wide access to data that supports department missions but require measures to ensure their confidentiality, integrity, and availability. The servers that host these resources must maintain the level of security mandated by department policy.

Systems within the headquarters' enterprise Active Directory domain are not fully compliant with the department's security guidelines, and no mechanism is in place to ensure their level of security. These systems were added to the headquarters domain, from trusted components, before their security configurations were validated. Allowing systems with existing security vulnerabilities into the headquarters domain puts department data at risk of unauthorized access, removal, or destruction.

Also, the department does not have a policy to verify the quality of security configuration on component systems that connect to headquarters. Interconnection security agreements are present for each connection between headquarters and components to secure shared services; however, neither the agreements nor other policy define specific security controls required for connecting systems. Stronger management and technical controls are needed on trusted systems to protect data provided by the department's enterprise-wide applications.

We are making three recommendations to the Office of Chief Information Officer. The Office of Chief Information Officer concurred with all recommendations and has already initiated actions to implement them. The Office of Chief Information Officer's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

Active Directory provides authentication services on a network. It allows system administrators to assign security policies, deploy software, and apply critical software updates to the organization's Windows servers and workstations. Administrators organize information technology resources into logical groups of computers and users, or Active Directory domains, to facilitate security and systems management.

Across the Department of Homeland Security (DHS), Active Directory has been implemented under a federated model where policy and guidance are centrally promulgated, but each component is responsible for its own network operations. Major components of DHS manage and control their own Active Directory domains, each with their own users, groups, workstations, and servers, and remain wholly separate from the headquarters domain, as shown in Figure 1.¹

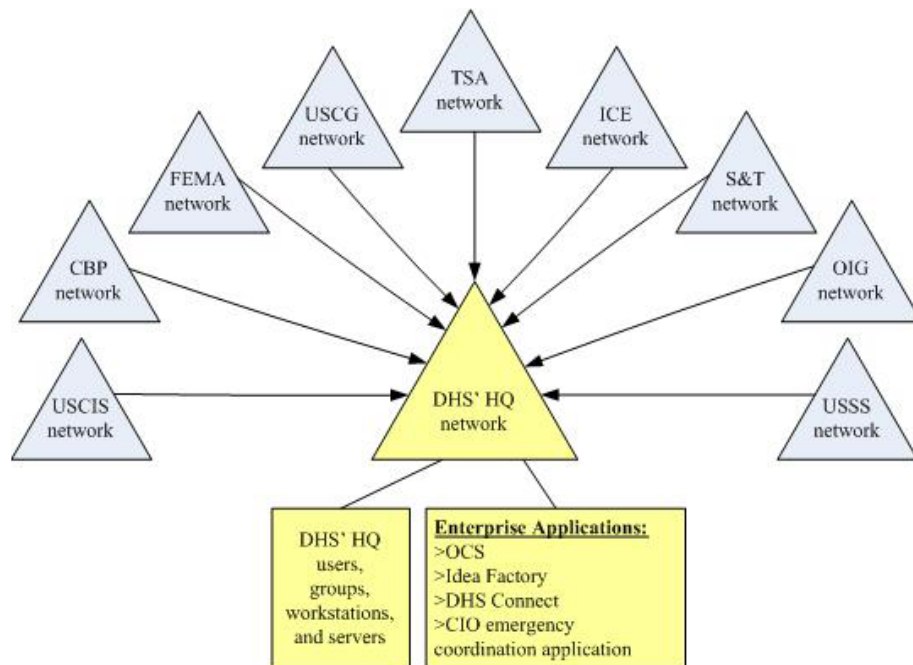


Figure 1. DHS' Headquarters Active Directory Connections

¹ The following components have Active Directory connections with DHS headquarters: Customs and Border Protection (CBP), Federal Emergency Management Agency (FEMA), Immigration and Customs Enforcement (ICE), Office of Inspector General (OIG), Science and Technology (Directorate) (S&T), Transportation Security Administration (TSA), United States Citizenship and Immigration Services (USCIS), United States Coast Guard (USCG), and United States Secret Service (USSS).

Some programs, called enterprise applications, require access by users from more than one component and are configured to cross regular domain boundaries. Active Directory uses trusts, or logical connections, to allow users to access information outside their home domain without needing additional accounts on the external domain.

DHS has established trusts between the headquarters domain and nine other components' domains to grant disparate users access to centralized enterprise-wide applications. Some of the applications are owned by components, while some are owned by DHS and provided as a service to component users. For example, DHS recently deployed Microsoft Office Communications Server (OCS) on its headquarters domain. Users throughout the department access OCS for virtual conferencing and collaboration.

In February 2007, the Secretary issued a policy on internal information exchange and sharing intended to foster "one DHS." The policy envisions an information-sharing environment free of unnecessary limitations or constraints. The policy also highlights the need to ensure the integrity of ongoing operations and conduct practices in a manner consistent with the law, including federal privacy and information security requirements. DHS' deployment of enterprise applications on the headquarters domain shows progress toward achieving a "one DHS" information-sharing environment.

Results of Audit

Vulnerable Systems Added to DHS Network

DHS' implementation of Active Directory provides security controls for its systems and users, but these controls can be circumvented. Specifically, DHS has allowed systems to be connected to its network and added to its domain through its trusts with other components that do not comply with published security policy. Further, trusted systems do not meet the level of security stipulated by service agreements. As a result, systems with vulnerabilities could allow unauthorized access and service disruption to the department's critical enterprise applications.

The security of Active Directory services comes from policy, the implementation of guidelines, and the use of written agreements to govern the connections. Failure to enforce policy and the poor quality of security configuration implementation on servers added to DHS' headquarters domain from other components puts department data at risk.

We reviewed servers in the enterprise application domain to determine the level of compliance with published Active Directory security configuration policy. Systems from CBP, ICE, and S&T contained security vulnerabilities and do not have configuration controls specifically identified within the DHS Sensitive Systems Policy Directive 4300A and Handbook and the DHS Secure Baseline Configuration Guide for Microsoft Windows. These vulnerabilities leave servers and, consequently, the department's headquarters domain and network at risk.

Examples of vulnerabilities include:

- A default privileged account enabled on a Windows server
- Missing security patches
- Local password policy not set to DHS standards
- A protocol in use that is specifically identified in DHS policy as vulnerable.

DHS 4300A outlines security controls that provide automated protection against unauthorized access or misuse. DHS 4300A facilitates detection of security violations and supports security requirements for applications and data on DHS systems. The policy directive includes controls specifying the local password policies, privileged account management, and the requirement to apply security patches in a timely manner. Additionally, DHS' secure baseline configuration guides provide system administrators with a set of procedures that will ensure a minimum security baseline when installing or configuring a Microsoft Windows server. Configuration settings within the Microsoft Windows server guide directs administrators to refuse protocols that are currently in use on some trusted systems.

While Active Directory provides security controls for systems and users, these controls are not inherited by systems added to its enterprise application domain. A basic tenet of information security is to apply controls to systems that not only exist within a network, but to those that connect to it as well. By accepting trusted systems from other components without enforcing or confirming security controls, DHS exposes its network to vulnerabilities contained on those systems. Risks associated with these vulnerabilities include potential unauthorized access to data or interruption of critical services to both DHS employees and the public.

Services that require enterprise-wide access need at least the same level of security controls as those systems contained within components' domains. We determined, however, that component-owned systems hosted on the headquarters domain are not fully compliant with DHS security policy. Moreover, DHS does not ensure that trusted systems meet information security requirements before allowing connectivity to its network.

The current implementation of Active Directory does not have controls to secure the systems put in place to support the requirements of enterprise applications. Initially designed to support only headquarters, the current Active Directory structure is not optimized for supporting enterprise-wide applications. To secure the systems that are added, manual procedures and individual validations must be performed. These processes have not proven to be effective in maintaining the level of security required on DHS' network. The department has recently undertaken efforts to better organize the department's Active Directory security framework to better support enterprise applications and offer components more efficient access to critical data.

Governance Needed to Verify Security Requirements

DHS has not established policy to enforce the implementation of security controls on component systems. Currently, DHS uses interconnection security agreements (ISA) to establish individual and organizational security responsibilities for the protection and handling of sensitive but unclassified information between DHS' headquarters domain and the component domain. However, while the ISA documents in place for headquarters and components describe policy, they do not provide specific measures, such as audits or vulnerability assessments, for either party to validate security controls on connected systems and enforce any needed changes. As a result, the ISAs exist only as an agreement to adhere to DHS policy.

DHS requires that an ISA identify roles and responsibilities for policy and guidance enforcement. An ISA should contain language to identify how security controls are implemented to protect the confidentiality, integrity, and availability of the data and systems being interconnected.

Conclusion

Regardless of the approach DHS takes in moving forward with its Active Directory restructuring, security policy implementation and enforcement must be considered as an integral part of any project that could expose DHS systems and data to risk. While DHS continues to speed the deployment of state-of-the-art systems and strive for "one DHS" as directed by the Secretary, it cannot sacrifice the confidentiality, integrity, or availability of its data and services. DHS' current Active Directory trusts pose risks and require stronger security controls in place to provide secure and effective enterprise services.

Recommendations

We recommend that the Chief Information Officer:

Recommendation #1: Verify that security controls are implemented and configuration settings are compliant with DHS policy on systems connected or added to DHS' Active Directory enterprise application domain through trusts.

Recommendation #2: Address the current vulnerabilities on systems connected to Active Directory.

Recommendation #3: Provide governance to ensure appropriate security measures are taken for all systems.

Management Comments and OIG Analysis

The Office of Chief Information Officer (OCIO) concurred with recommendation 1. The Active Directory Working Group will work with the Security Policy Working Group of the Chief Information Security Officers Council to develop guidance for Active Directory configurations.

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

The OCIO did not concur with recommendation 2 as written in the draft report. The OCIO suggested revised recommendation language that it believed would better address what the report is targeting. We agree with OCIO and have revised some of the language as suggested. OCIO concurs with revised recommendation 2, and is working to address the vulnerabilities identified.

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

The OCIO did not concur with recommendation 3 as written in the draft report. The OCIO suggested revised recommendation language and we agreed to this change. OCIO concurs with revised recommendation 3, and is taking corrective actions to address the deficiencies identified.

We agree the steps that OCIO is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved and it

will remain open until OCIO provides documentation to support that all planned corrective actions are completed.

OCIO also provided technical comments on the report, and we have incorporated these comments where appropriate.

Appendix A

Purpose, Scope, and Methodology

The objective of our review was to determine whether DHS has implemented effective security controls on its Active Directory domain. We conducted this performance audit between September 2009 and January 2010 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, Information Technology Audits, at (202) 254-4041 and Chiu-Tong Tsang, Director, Information Security Audit Division, at (202) 254-5472.

Appendix B

Management Comments to the Draft Report

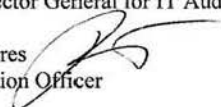
U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

March 29, 2010

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General for IT Audits

FROM: Richard A. Spires 
Chief Information Officer

SUBJECT: OIG Draft Response: "Stronger Security Controls Needed on Active Directory"

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, "Stronger Security Controls Needed on Active Directory." The OCIO response to the OIG recommendations is as follows:

Recommendation #1: Verify that security controls are implemented and configuration settings are compliant with DHS policy on systems connected or added to DHS' Active Directory enterprise application domain through trusts.

OCIO March 2010 Response: OCIO concurs. The Active Directory Working Group will work with the Security Policy Working Group of the Chief Information Security Officers Council to provide guidance that will allow clear direction for Active Directory (AD) configurations.

Recommendation #2: Ensure that existing vulnerabilities on trusted systems are not carried forward with any changes to the headquarters Active Directory services.

OCIO March 2010 Response: OCIO does not concur. The second recommendation does not appear to address what the report is targeting. OCIO proposes the following language instead: "Ensure that current vulnerabilities are addressed and that processes, procedures and governance be instituted to ensure that DHS Enterprise Authentication services meet the mission needs."

Recommendation #3: Revise the Interconnection Security Agreement (ISA) document to provide a mechanism for DHS to validate the security controls and configuration settings on systems before they are connected or added to DHS' headquarters domain.

OCIO March 2010 Response: OCIO does not concur. As part of the existing ISA, pursuant to DHS 4300A policies and as controlled by the Infrastructure Change Control Board (ICCB), all systems that interconnect with AppAuth must have an Authority to Operate (ATO). In addition, each system

Appendix B

Management Comments to the Draft Report

must have an Information Systems Security Officer who is personally responsible for ensuring that the systems meet the security requirements and providing that assurance on the change that connects the application to AppAuth.

OCIO suggests that Recommendation #3 be revised to read: "Provide Governance such that appropriate security measures are taken for all systems."

Appendix B

Management Comments to the Draft Report

In addition, OCIO also offers the following comments throughout the February 2010 report "Stronger Security Controls Needed on Active Directory Systems":

#	Draft Report Section	DHS Comment
1	P. 1, first paragraph, "In particular, we evaluated the security of the Active Directory collection of enterprise resources and services used by components across the department through trusted connections."	<p>The document refers to the issues within the Headquarters' Enterprise Active Directory (AD). This language could be confusing since the Headquarters has its own AD domain called "DHSnet" that supports the DHS Headquarters Sensitive-but-Unclassified office automation network referred to as "LAN-A," which is separate from the DHS Enterprise Active Directory also known as "AppAuth." OCIO suggests using Enterprise Authentication or AppAuth to help keep the context clear.</p> <p>OIG: No change. For purposes of this report we do not believe it is necessary to define the Headquarters' AD structure in terms of root and child domains.</p>
2	P. 1, second paragraph, "Overall, systems within the headquarters' enterprise Active Directory domain are not fully compliant with the department's security guidelines, and no mechanism is in place to ensure their level of security."	<p>OCIO agrees that AppAuth needs to be improved. In fact on December 16, 2009 the CIO/CISO community endorsed a general upgrade plan for DHS. This plan is highlighted below:</p> <p><u>Major Milestone for AppAuth V2.0 (NextGen):</u></p> <ul style="list-style-type: none"> • Establish AD Working Group - (completed) • Determine how U.S. Coast Guard (USCG) and U.S. Secret Service (USSS) should integrate into AppAuth • Implement Governance Model For AppAuth and Enterprise Federated AD • Create AppAuth Development and Test Environment • Upgrade all Enterprise facing DC's to 2008R2 • Implement two way trust • Create resource forest for all ofDHS in AppAuth (dynamic entries) • Create tools to populate and maintain enterprise Forest in AppAuth • Obtain revised ATO for AppAuth NextGen <p>This investment by DHS will provide the robust governance called for in the OIG draft report and improve integration and data sharing throughout the Department. DHS has already made improvements by eliminating Windows Server 2000 Domain Controllers in one Component's domain, which were unsupportable, by (1) obtaining improved hardware for AppAuth, (2) providing monitoring of the AppAuth communications and infrastructure, and (3) integrating USSS into the Trust.</p> <p>OIG: No change. We agree that the steps OCIO is taking will strengthen the controls implemented on AppAuth.</p>
3	P. 1, third paragraph, "...the interconnection security agreements between headquarters and components to properly secure their shared services, are current for each connection present,	<p>As identified and defined with the DHS 4300A security policy, ISAs are agreements on how connections between systems will be developed and sustained. The ISA is not intended as the enforcement tool; but rather a method for the stakeholders (the Approving Officials for the connecting systems) to identify mutual areas of risk and the appropriate controls to mitigate those risks. Recognizing that the ISA is not the appropriate mechanism to address the items of concern as identified by the OIG, we suggest that DHS use its Governance processes that are being stood up</p>

Appendix B

Management Comments to the Draft Report

	but containing no provisions to ensure the quality of security configuration on the systems.”	<p>under the Information Technology Services Governance Board (ITSGB) to ensure that Authentication Services are correctly implemented and sustained. From CISO governance considerations, there are ongoing activities to allow enterprise service offerings to provide clearer guidance on the specifics of the services provided (specifically on the NIST 800-53 controls) and the requirements for systems to interconnect to the enterprise service. It is expected the AppAuth will be a prime example of this Enterprise Security Service Agreement in lieu of multi-party ISAs.</p> <p>OIG: We revised the report to note that there is no governance in place to verify the security of controls on component systems that connect to headquarters.</p>
4	P. 2, first paragraph, “Active Directory allows system administrators to assign security policies, deploy software, and apply critical software updates to the organization’s Windows servers and workstations.”	<p>Active Directory provides authentication services. It is used by systems to facilitate patching and software delivery, but does not do these items itself.</p> <p>OIG: We revised the report to clarify that “Active Directory provides authentication services on a network,” and “it allows system administrators to assign security policies, deploy software, and apply critical software updates to the organization’s Windows servers and workstations.”</p>
5	P. 2, second paragraph, “Across the department, Active Directory has been implemented under a federated model where policy and guidance are centrally promulgated, but each component is responsible for its own network operations.”	<p>The performance of network operations is separate and distinct from the management of Active Directory. Active Directory Policies and Services are managed by the Components in a federated model. Federation is actually Microsoft’s Best Practice approach to diversified organizations’ use of Active Directory. However, DHS would like to improve the governance of the group policies and management of these federated active directories.</p> <p>OIG: No change.</p>
6	P. 2, Figure 1, “DHS’ Headquarters Active Directory Connections”	<p>A blue triangle should be added for LAN-A (DHSnet), which is the Headquarters Active Directory domain, and the yellow triangle should read Enterprise Authentication (AppAuth).</p> <p>OIG: No change.</p>
7	P. 2, Figure 1, “DHS’ Headquarters Active Directory Connections”	<p>Currently, there are 10 domains that AppAuth integrates. FLETC should be included as well. Also please note that TSA includes the Federal Air Marshal Service and Federal Flight Deck Officer program.</p> <p>OIG: No change. In December 2009, OCIO identified 10 components with trusts in place with Headquarters. FLETC was not included in the 10 identified. Additionally, no change was made regarding the Federal Air Marshal Service and Federal Flight Deck Officer since they are programs under TSA.</p>
8	P. 3, second paragraph, “...DHS recently deployed Microsoft Office Communications Server (OCS) on its headquarters domain. Users throughout	<p>Office Communication Service (OCS) was deployed in AppAuth. There was an element of the enterprise OCS deployment that also required the Component controlled AD domains to perform concurrent activities to assure proper operation.</p>

Appendix B

Management Comments to the Draft Report

	the department access OCS for virtual conferencing and collaboration.”	OIG: No change.
9	P. 5, first paragraph, "Moreover, DHS does not ensure that trusted systems meet information security requirements before allowing connectivity to its network. "	<p>The sentence is not accurate. As part of the existing ISA, pursuant to DHS 4300A policies and as controlled by the ICCB, all systems that interconnect with AppAuth must have an ATO, and each system must have an ISSO who is personally responsible that the systems meet the security requirements and who provides assurance on the change that connects the application to AppAuth.</p> <p>OIG: No change. While we acknowledge that DHS policy designates an ISSO as responsible for system security requirements, we maintain that there is no governance in place for OCIO to verify the security of controls on component systems that connect to headquarters.</p>

Appendix C

Major Contributors to This Report

Information Security Audit Division

Edward Coleman, Director

Chiu-Tong Tsang, Director

Mike Horton, Information Technology Officer

Amanda Strickler, Information Technology Specialist

Frederick Shappee, Referencer

Appendix D
Report Distribution

Department of Homeland Security

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

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate



ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
DHS Office of Inspector General/MAIL STOP 2600,
Attention: Office of Investigations - Hotline,
245 Murray Drive, SW, Building 410,
Washington, DC 20528.

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