U.S. DEPARTMENT OF THE INTERIOR

OFFICE OF INSPECTOR GENERAL

Evaluation of Information Technology System Configuration

ISD-EV-MOA-0003-2009

September 2009

Contents

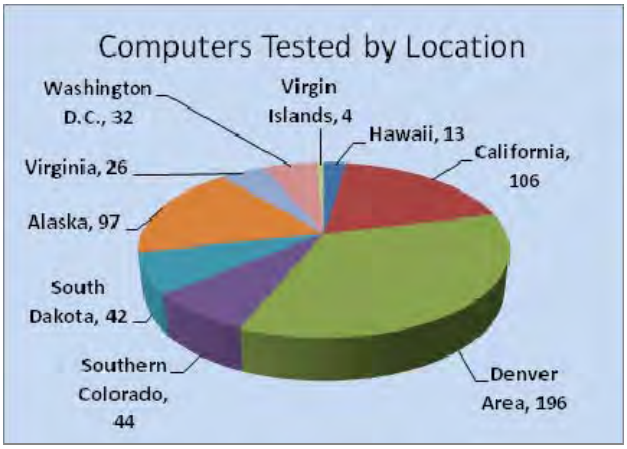
Acronyms and Other Reference Terms

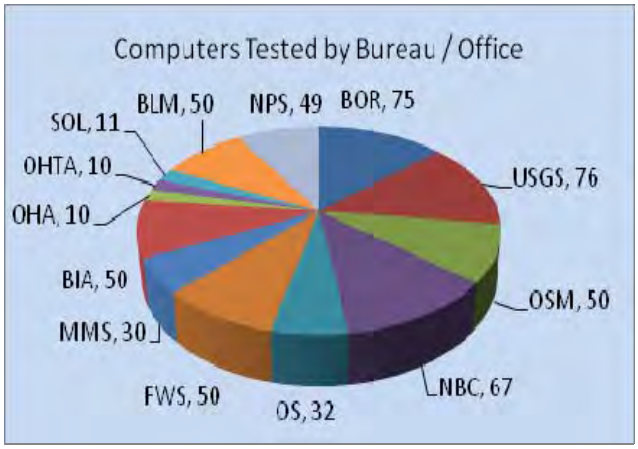
BLM.....Bureau of Land Management
BOR ..... Bureau of Reclamation
BIA.....Bureau of Indian Affairs
CIGIE.....Council of Inspector General on Integrity and Efficiency
CIO.....Chief Information Officer
CISO .....Chief Information Security Officer
CIRC ..... Computer Incident Response Capability
CSD.....Cyber Security Division
Department..... Department of the Interior
DOD..... Department of Defense
DOI ..... Department of the Interior
DHS..... Department of Homeland Security
DSL .....Digital Subscriber Line
EAD .....Enterprise Active Directory
EEO.....Equal Employment Opportunity
FDCC .....Federal Desktop Core Configuration
FISMA ..... Federal Information Security Management Act
FWS ..... U.S. Fish and Wildlife Service
GAO.....Government Accountability Office
HQ..... Headquarters
IE6..... Internet Explorer 6
IE7..... Internet Explorer 7
ISD ..... Information Security Division
IT..... Information Technology
LE.....Law Enforcement
MMS ..... Minerals Management Service
NPS ..... National Park Service
NBC .....National Business Center
NIST.....National Institute of Standards and Technology
NPS ..... National Park Service
OCIO……..….....Office of the Chief Information Officer
OS .....Office of the Secretary
OIG ..... Office of Inspector General
OMB .....Office of Management and Budget
OSM.....Office of Surface Mining
OHA..... Office of Hearing and Appeals
OHTA .....Office of Historical Trust Accounting
SCAP.....Security Content Automation Protocol
SOL..... Office of Solicitor
USGS ..... United States Geological Survey

Background

The Federal Information Security Management Act (FISMA) requires agencies to comply with standards to secure information and information systems. In March 2007, the Office of Management and Budget (OMB) directed agencies to comply with security configuration standards developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DOD), and the Department of Homeland Security (DHS). These standards became the Federal Desktop Core Configuration (FDCC). In its March 20, 2007 memorandum, OMB directed agencies to comply with FDCC standards by February 1, 2008. In March 2008, the Department's Office of Chief Information Officer issued policy requiring all offices to be in full compliance with the FDCC standards by September 30, 2008. OMB's August 2008 memorandum, M-08-22, *Guidance on the Federal Desktop Core Configuration*, directed agencies to meet or exceed FDCC standards regardless of the function of their workstations.

We conducted our evaluation between April and July 2009. We tested 560 computers with the Windows XP Operating System across the Department.





We conducted three tests on every computer sampled: Windows XP Operating System, Internet Explorer Version 7 (IE7), and the Windows XP firewall. We utilized an available SCAP[1]-compliant commercial off-the-shelf product to perform our testing.

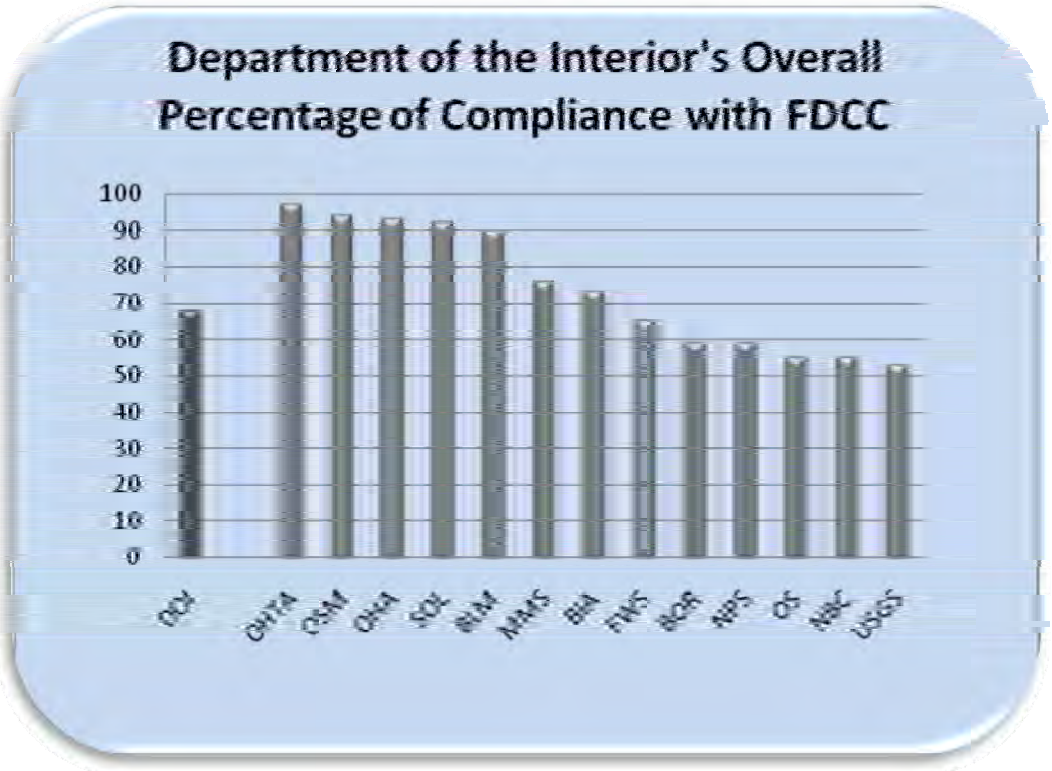
[1] Security Content Automation Protocol (SCAP) compliant software follows NIST's guidance and allows specific standards to be used to measure compliance.

Results In Summary

We found widespread noncompliance with mandatory FDCC standards and noncompliance with directives issued by the Department's Chief Information Officer (CIO). We also found substandard conditions in bureau server rooms, unauthorized network circuits, and unauthorized network equipment. Our testing revealed a lack of standardized software across the Department and frequent use of escalated user privileges (i.e., Administrator or Power User). Many issues resulted from a lack of management and Departmental oversight.

Our testing determined the Department is 68 percent compliant with mandatory FDCC settings. Within the Department, five offices averaged 90 percent or higher, three offices averaged between 60 percent and 75 percent, and five offices averaged below 60 percent. Computers that were not centrally managed were 45 percent compliant with mandatory FDCC settings.

> "The standardized desktop configuration effort began in 2003 when the USAF implemented a single, gold-standard configuration for their workstations…This standardized configuration has now been deployed to an estimated 500,000+ workstations and has directly resulted in a 30 percent reduction in IT management costs."
>
> —NetIQ, November 19, 2008

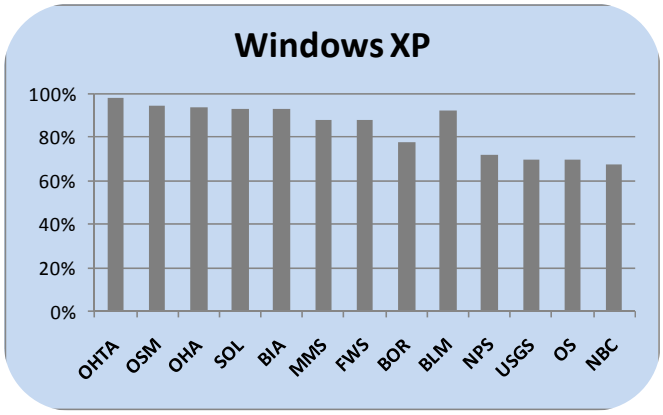


In November 2008, the Government Accountability Office (GAO) initiated a review of three federal information security initiatives at 24 federal departments and agencies. One initiative was the FDCC. As part of their audit, GAO requested compliance information from the Department. Our review of the data revealed the Department acknowledged 61 percent (50,935 computers) of their Windows XP and Vista desktops and laptops were not compliant with FDCC. Less than half the offices within the Department used a SCAP-compliant tool to test for FDCC compliance.

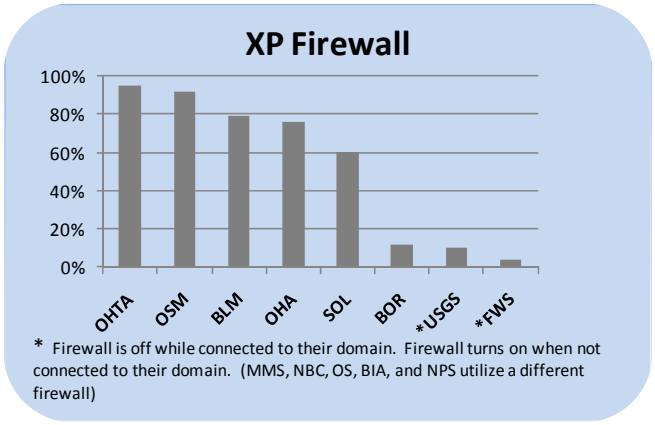
Noncompliance with mandatory standards, use of unauthorized network circuits, and use of unauthorized network hardware are a direct threat to Departmental missions. Electronic data necessary to conduct and support missions are stored and processed by at-risk information systems. Compromising these information systems could affect the integrity of the Department's electronic data and its backup copy. Some electronic data stored or processed on these systems may be irreplaceable. If data stored or processed on these information systems were manipulated and went undetected, irreparable damage could severely inhibit Departmental operations.

Compliance with Configuration Requirements

The FDCC benchmarks we evaluated for compliance were Windows XP Professional, IE7, and the Windows XP firewall. Since software was not standard across the Department, we found some offices used different products or versions. For example, IE7 was being tested and deployed in some offices while in others it had been fully deployed and operational for months. Five offices did not use the Windows XP firewall. Lack of standardization makes monitoring and oversight more difficult and raises support costs.



Windows XP Professional
We tested 342 configuration settings on each computer sampled for the Windows XP benchmark. We sampled 560 workstations and found an average compliance rate of 80 percent. See Appendices 3 and 4 for details.



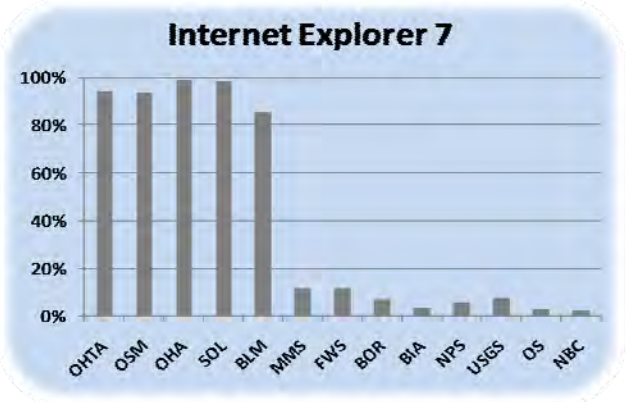
Windows XP Firewall
We tested 25 configuration settings on each computer sampled for the Windows XP firewall benchmark. We sampled 560 workstations and found 206 did not have the Windows XP firewall enabled or configured. Of the 354 computers using the Windows XP firewall, we found the compliance rate was 54 percent.

U.S. Fish and Wildlife Service (FWS) and United States Geological Survey (USGS) disabled the Windows XP firewall while connected to their own network and configured the firewall to automatically enable when connected to a network other than their own. We tested this functionality in FWS and found it worked as configured. We tested this functionality in USGS and found it worked with the exception of one office in Sacramento, CA. The local administrator changed the security settings affecting 115 laptop computers prior to our arrival, thus the firewall never enabled as designed. Even when enabled, the firewall was 10.4 percent compliant across USGS and 4 percent compliant across FWS. Individual workstations without a firewall leave computer systems and information vulnerable to threats. The 2008 Computer Security Institute Computer Crime and Security Survey reported 44 percent of incidents were from insider network abuse. Regardless of FWS and USGS' designs, FDCC mandates the use of a firewall.

While NIST guidelines permit agencies to use other desktop firewall software besides the Windows XP firewall, we did not find Departmental guidance on a standard desktop firewall. FWS installs firewalls on laptops that use wireless Internet, and USGS allows each site to choose for itself between the Windows XP firewall and Symantec's firewall product. Minerals Management Service (MMS), National Business Center (NBC), Office of the Secretary (OS), Bureau of Indian Affairs (BIA), and National Park Service (NPS) also utilized other firewall products in lieu of the Windows XP firewall. The lack of standardization increases costs of system management and impairs the Department's ability to perform oversight.

Internet Explorer Version 7

We tested 100 configuration settings on 560 workstations and found 37 did not have IE7 installed. Of the 523 with IE7, the average compliance rate was 29 percent.



NIST recommends IE7 if the IE browser is used. Some bureaus still use IE Version 6. Other applications for web browsing, such as Firefox, were installed on workstations where IE7 or IE6 were already installed. Lack of standardization increases operating costs, makes support more difficult, and impairs oversight. We found no Departmental configuration guidelines for other web browsing products and saw no evidence that mandatory configuration settings had been adopted for these other web-browsing products.

We manually reviewed additional FDCC requirements along with FDCC benchmarks. For example:

Least Privilege

Least privilege is a principle in computing that states a user should only be given privileges necessary to perform their job. Mandatory FDCC settings prohibit assigning escalated privileges to end-users. Many users were assigned escalated privileges (i.e., "Administrator" or "Power User") to their workstations. FWS and MMS routinely assigned escalated privileges. According to NIST, any privilege that is not a default user right is an "escalated privilege."[2]

Wireless Networking

We found laptop computers connected to bureau networks with wireless interfaces enabled at USGS. There is high risk that these laptop computers could accidentally connect to an unauthorized wireless access point and create access to the Department's network.

Continuous Monitoring – Federal Information Processing Standard (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, requires agencies to monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls. The Department has almost no ability to monitor for

[2]NIST FDCC Technical Frequently Asked Questions, April 2009, Question #73 (http://nvd.nist.gov/fdcc/fdcc_faq.cfm)

FDCC compliance due to many bureaus electing not to connect their Enterprise Active Directory (EAD) infrastructure to the Department's central reporting capability.

We found some computers managed separately from the EAD. Those individually managed computers averaged only 45 percent compliant with mandatory FDCC settings. Offices cannot solely rely on EAD to manage compliance when computers can connect to their network without mandatory EAD participation. Examples of individually managed computers include:

- BLM - A law enforcement computer connected directly to the Internet to perform background checks. The computer was perpetually logged in as Administrator, had no anti-virus software installed, and no supplemental network security between it and the Internet (56 percent compliance with FDCC).
- Bureau of Reclamation (BOR) – A computer used to manage building access to a facility in Durango, CO (53.9 percent compliance with FDCC).
- NBC – A computer used to manage building access to facilities in Lakewood, CO (31 percent compliance with FDCC).
- NPS – A computer used to bypass the Enterprise Services Network (ESN) to allow users access to social networking websites (48 percent compliance with FDCC).
- OS – One user managed his own FDCC settings while connected to the Department's network (47 percent compliance with FDCC).
- USGS – A computer designated as a "visitor" computer connected directly to the Internet via a digital subscriber line. It had no anti-virus software installed (41 percent compliance with FDCC).

Deviation from Requirements

OMB policy recognizes that agencies might determine that some settings in the FDCC are not practical. The Department's Office of the Chief Information Officer (OCIO) Directive 2007-001, *Security Technical Implementation Guide (STIG) for Windows XP*, contains specific guidance and procedures for accepting the risk for FDCC deviations:

> "...weaker security settings should be addressed through either (1) the development of appropriate corrective action plans and documented in the appropriate program- or system-level Plan of Action and Milestones (POA&M) or (2) through formal documentation, acknowledgement, and acceptance of risk by the responsible Designated Approving/Authorizing Authority (DAA). Risk acceptance requires written and signed concurrence from the DOI CIO."

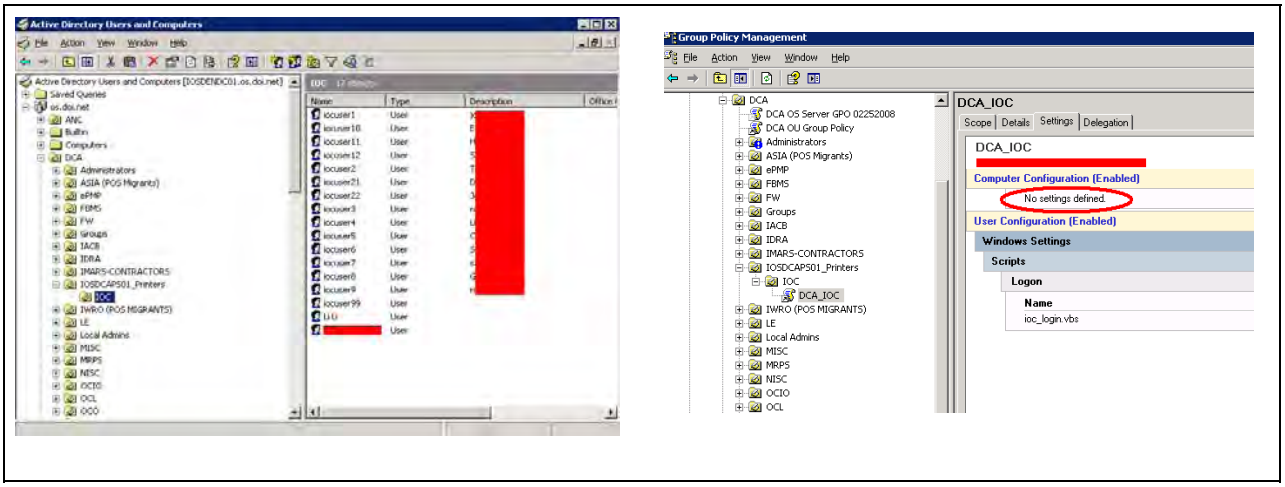
The directive further explains the process for requesting deviations.

In May 2009, the Department released an approved list of four Department-wide FDCC deviations. Offices reported an additional 323 deviations from the FDCC mandate; however, we found no approved deviations documented in accordance with OCIO Directive 2007-001. The Solicitor's Office (SOL) identified eight deviations with no associated Plan of Action and

Milestones (POA&M). All other offices had POAMs for deviations or stated they were in the process of creating them.

Bureau / Office	Number of Reported Deviations	Bureau / Office	Number of Reported Deviations
BIA	5	**OHA**	0
BLM	20	**OHTA**	46
BOR	188	**NPS**	4
FWS	4	**OSM**	4
MMS	17	**SOL**	10
NBC / OS	23	**USGS**	2

In our review of the OS Domain of Active Directory, we found 17 user accounts grouped in an area normally reserved for printers. We reviewed this group of user accounts and found FDCC settings were not applied. There were no approved deviations submitted for these 17 user accounts.



February 1, 2008 was OMB's deadline for federal agencies to be compliant with FDCC standards. The Department does not have all deviations formally documented and is less than 70 percent compliant with the FDCC mandate.

Oversight

The Department's Cyber Security Division is responsible for performing oversight but lacks the necessary resources and expertise to conduct oversight functions such as inspections, technical testing, and monitoring. Lack of oversight is a significant weakness in the Department's overall information systems security program.

Department Manual, Part 18, Paragraph 18.5(A)1 requires the Department's "Information Technology Security Staff" (i.e. Cyber Security Division) to perform "oversight." In addition, Department Manual, Part 375, Chapter 19, Paragraph 19.8(D)10 requires the Department Chief Information Security Officer (CISO) to oversee "bureau compliance with Federal and Departmental policies, guidelines, and regulations governing IT security."

In 2006, the Department CISO developed the *Cyber Security Major Reorganization Plan* (Plan). The Plan included a "Compliance and Oversight Division" consisting of 11 fulltime employees. The Plan stated, "The Compliance and Oversight Division provides independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures." The Plan, ultimately, was not approved.

The Department's IT Strategic Plan Fiscal Year (FY) 2007 – FY 2012 describes the EAD as a "single authoritative user directory for controlling access to IT systems and services." We found EAD frequently used by offices to apply FDCC settings. We further found that between FY 2008 and FY 2009, the Department spent $960,000 to enable audit logging and event alerting capabilities, which are fundamental elements of monitoring and oversight activities. The first milestone was scheduled to be completed by March 31, 2009, however, as of July 21, 2009, we found:

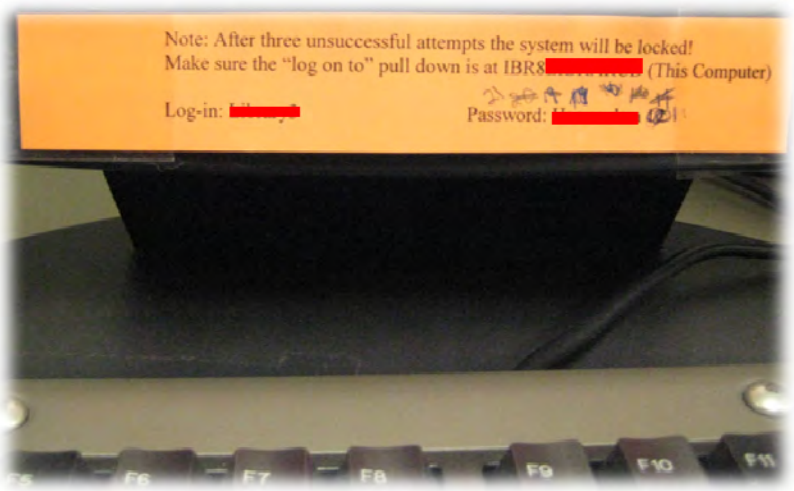
- Office of the Solicitor was 80 percent connected
- Office of Special Trustee was 50 percent connected
- Office of Hearing and Appeals was 50 percent connected
- Office of Historical Trust Accounting was 50 percent connected
- National Business Center was 16.67 percent connected
- Bureau of Indian Affairs was 9.09 percent connected
- Minerals Management Service was 0 percent connected
- National Park Service was 0 percent connected
- Office of the Secretary was 0 percent connected
- United States Geological Survey was 0 percent connected

On July 1, 2009, we observed a meeting related to EAD. During the meeting, staff from the Department asked the MMS representative why MMS was not connected to the Department's central servers. The MMS representative responded, "We don't want you to have that information."

Other Observations

We found widespread lack of standardization and noncompliance with OMB policy and Department CIO directives. For example, we found unauthorized network circuits and network hardware, usernames and passwords taped to monitors, personally owned software installed on government-owned computers, and substandard server rooms. Not all mobile devices were encrypted as required by OMB M-06-16, *Protection of Sensitive Agency Information*.

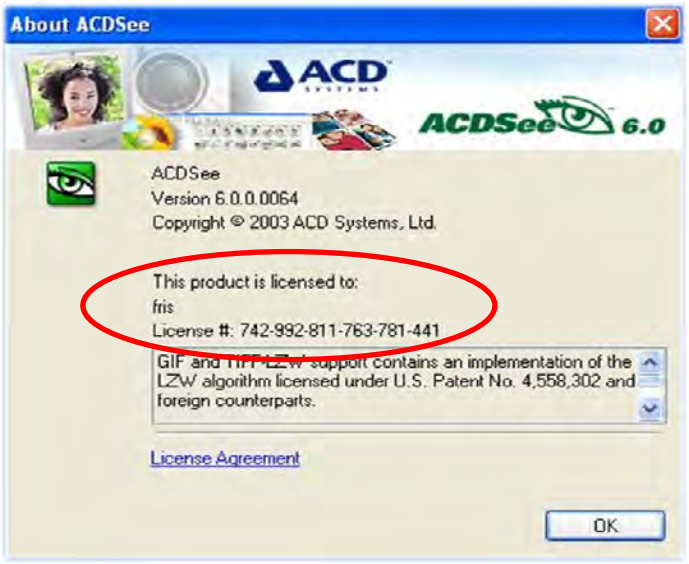
We found workstations in MMS, BLM, and BOR with the username and password posted directly on a monitor. This picture shows a publicly accessible computer in the BOR Library, Lakewood, CO.



The OS reported they "do not maintain any desktops as that is a service fully provided by NBC." Conversely, nine computers in Denver, CO, had FDCC settings maintained by OS. One was managed solely by an OS employee who had escalated privileges.

In SOL's response to the GAO, they claimed to use a SCAP-compliant tool called "Secutor Prime" to verify FDCC settings. When we contacted the vender, they stated they had provided an evaluation copy to SOL for testing purposes and the evaluation key expired earlier in 2008. The vendor confirmed SOL had not purchased the product as of July 26, 2009. The vendor acknowledged the free version of their product was not SCAP-compliant as required by NIST.

We found personally owned software installed on a workstation in FWS in Sacramento, CA.



While reviewing the results from BOR, we found computers with Internet (public) routable IP addresses. This is not consistent with best practice and is detrimental to information security because internal addresses are not masked to an external observer.

We found several network circuits that bypassed the Department's ESN, which provides extensive technical security capabilities to enhance protection beyond what individual computers could provide for themselves. Forgoing the protection provided by ESN and connecting directly to the Internet is risky. The Department CIO ordered all bureau and office networks to connect to ESN by August 16, 2005. We found unauthorized network hardware used to provide remote access and server rooms that failed to meet best practices for securing and protecting information systems.

The unauthorized circuits we found included:

- A network circuit providing the BLM Law Enforcement (LE) Office in Sacramento, CA, with Internet connectivity. The sole computer connected to this circuit was noncompliant with mandatory FDCC configuration guidance, had no virus protection, did not have a firewall, and was constantly logged in as the Administrator. BLM LE personnel said this computer was used to perform background checks as well as verify information such as vehicle license plates and registration. This setup posed a substantial risk of losing personally identifiable information. We immediately notified the Department CISO by telephone.
- A network circuit providing NPS with Internet connectivity at Mount Rushmore National Park. We scanned this circuit and found misconfigured network hardware as well as a vulnerable server. This circuit was disconnected within weeks of us reporting it to the Department.

- A network circuit providing BLM with Internet connectivity at the Sacramento, CA office. BLM personnel stated they used this circuit to connect to social networking sites on the Internet that were blocked by the Department's web filter. One of the computers using this circuit had not had its virus protection updated in more than 6 months. Updates to virus protection software normally occur daily.

We found network circuits providing BLM, FWS, NPS, and MMS offices in Anchorage, AK, with Internet connectivity. This picture shows a digital subscriber line connected to a workstation at FWS in Anchorage, AK.

- In Sacramento, CA, we found an unauthorized Virtual Private Network server used to provide remote access to BOR. The Department's CIO ordered all remote access servers disconnected by January 31, 2007.
- A network circuit providing the BLM office in Denver, CO, with Internet connectivity. BLM personnel claimed to have a waiver to maintain the circuit but were unable to provide a copy.

On October 1, 2006, the Department CISO sent a memorandum to the BLM CIO in which he stated, "Under my authority as Chief Information Security Officer (CISO) of the Department of the Interior to ensure agency compliance with the Federal Information Security Management Act (FISMA) and Departmental IT security policies and standards, and as directed by the authority of the Chief Information Officer of the Department of the Interior, the Bureau of Land Management is hereby ordered to… immediately disconnect all unapproved and unauthorized external circuits and gateways."

The substandard server rooms we found included:

The BOR server room in Sacramento, CA, was separated from adjacent work areas by only a mesh fence that did not go from floor to ceiling. The server area itself, as well as the adjacent work area, had substantial amounts of cardboard, wood, and other combustible material.

The FWS server room in Anchorage, Alaska, had a bucket located over the network equipment and electrical outlets to catch water.

Recommendations

To address the deficiencies identified in this report, we recommend:

1. Consider adding qualified information security inspectors to the Department's Cyber Security Division.
2. Fully leverage existing technology such as EAD to enable Departmental oversight.
3. Include compliance with OMB and Departmental policy as a performance objective on IT manager's annual performance report.
4. Comply with FDCC guidance for computer configuration.
5. Comply with NIST guidance for least privilege: remove end users' Administrator and Power User permissions.
6. Comply with OMB guidance for encrypting data on mobile computers.
7. Improve server room environments by consolidating equipment in facilities designed to house computer equipment.
8. Standardize software products so that monitoring and oversight is easier and support costs are lower.

Appendix 1: Objective, Scope, Methodology, and Other Related Coverage

Objective, Scope, and Methodology

Our objective was to assess the progress of implementing mandatory guidance for computer configuration across the Department.

We conducted our evaluation from April 29, 2009, to July 14, 2009. Our evaluation included records provided by the Department. In order to conduct technical testing, offices provided us with Administrator credentials to select computers. Some bureau and office personnel provided Administrative access.

In order to conduct tests, we used an available SCAP[3]-compliant commercial off-the-shelf products. Offices repeatedly claimed the product reported "false positives," which is when a misconfiguration is reported but does not actually exist. We invited the offices to provide evidence and examples of false positives but none were provided.

The results did not include the four approved deviations submitted by the Department as these deviations were not approved until after our fieldwork was underway. In order to provide consistency in reporting, we did not consider these deviations as many tests had already been completed. We did not consider any of the deviations submitted by offices as those deviations were not completed in accordance with OCIO memorandum 2007-001.

We conducted our evaluation in accordance with the *Quality Standards for Inspections* as put forth by the Council of Inspector General on Integrity and Efficiency. Accordingly, we included necessary record tests and other procedures. To accomplish our objective, we conducted the following activities:

- Reviewed applicable laws, regulations, OMB guidance, NIST standards, and Department and bureau policies
- Reviewed technical configuration of sampled computers
- Interviewed Department, bureau, and office information technology personnel
- Performed on-site inspections of offices

Other Related Coverage

The OIG issued *Compilation of Information Technology Challenges at the DOI*, dated May 2008, which documented the need for reform in the Department's management of information technology. Our office issued the annual FISMA evaluation report in September 2008 which documented organizational challenges and inefficiencies impeding information security across the Department.

[3] Security Content Automation Protocol (SCAP) compliant software follows NIST's guidance and allows specific standards to be used to measure compliance.

GAO Job Code 3110-14, *GAO Engagement: Review of Federal Information Security Initiatives*, commenced in November 2008. GAO's audit was conducted during the same time period as our evaluation. At the conclusion of our evaluation, GAO's audit report had not been released.

Report Fraud, Waste, Abuse And Mismanagement

Fraud, waste, and abuse in government concerns everyone: Office of Inspector General staff, Departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and abuse related to Departmental or Insular area programs and operations. You can report allegations to us in several ways.

By Mail:	U.S. Department of the Interior Office of Inspector General Mail Stop 4428 MIB 1849 C Street, NW Washington, D.C. 20240	
By Phone:	24-Hour Toll Free Washington Metro Area	800-424-5081 703-487-5435
By Fax:	703-487-5402	
By Internet:	www.doioig.gov	

Revised 06/08