AIR FORCE AUDIT AGENCY

COMPUTER NETWORK INCIDENT RESPONSE AND REPORTING

AUDIT REPORT

F2011-0004-FB4000

20 April 2011

INTRODUCTION

Incident response and reporting involves detection, timely reporting, containment, and analysis of all suspicious network activity. Suspect activity is first designated an "event" and investigated. Events confirmed as security breaches are designated '"incidents" and reported in the Joint Computer Emergency Readiness Team Database. The Air Force Computer Emergency Response Team (AFCERT) monitors Air Force network traffic and provides continuous real-time intrusion detection for over 150 installations. The AFCERT must identify and investigate all events, designate and report qualifying events as new incidents, and provide responsive corrective actions for each incident. From 1 January to 2 November 2009, the AFCERT investigated over 407 network events and reported 168 new incidents (hereafter referred to as cyber events and incidents).

OBJECTIVES

We performed this audit because prompt cyber event identification and responsive corrective action will reduce network vulnerability to malicious activity intent on degrading and disrupting network operation. The objective was to determine whether Air Force network personnel effectively managed cyber events and incidents. Specifically, we determined whether network personnel effectively:

- Investigated cyber events.
- Implemented corrective actions to prevent cyber incidents from recurring.

CONCLUSIONS

[redacted] Air Force network personnel did not effectively manage cyber events and incidents. Specifically, network personnel did not effectively:

- [redacted] Investigate all cyber events. Investigating cyber events is crucial for properly responding to and preventing future network attacks. (Tab A, page 1)
- [redacted] Implement corrective actions to prevent cyber incidents from recurring. Identifying and implementing corrective actions for cyber incidents improves the Air Force defense in-depth strategy to ensure networks are available to the warfighters. (Tab B, page 5)

[redacted]

RECOMMENDATIONS

We made four recommendations to improve cyber event and incident investigations and corrective actions to prevent future incident recurrence. (Reference the individual Tabs for specific recommendations.)

MANAGEMENT'S RESPONSE

Management concurred with the audit results and recommendations A.1, A.2, B.1 and B.2. Management comments were responsive, and actions planned should correct the problem. Therefore, this report contains no issues requiring elevation for resolution.

Judith L. Simon

BRUCE C. CARPENTER
Associate Director
(Cyber Security Assurance Division)

JUDITH L. SIMON
Assistant Auditor General
(Financial and Systems Audits)

Table of Contents

Tab A
Investigation

BACKGROUND

Cyber Events and Incidents. The AFCERT monitors Air Force network for suspicious activity. Three Air Force I-NOSCs[1] maintain operational control over all installation Network Control Centers (NCCs) and assist the AFCERT with event investigations. When the AFCERT identifies a cyber event, they request the I-NOSC identify the impacted computer(s) (called "true source"). The I-NOSC in turn forwards the request to the appropriate installation NCC to review firewall,[2] proxy server,[3] and domain name server (DNS)[4] audit logs to identify the impacted computer(s). The NCCs provide results back to the I-NOSC and AFCERT. The AFCERT then determines whether the event should be reported as an incident in the Joint Computer Emergency Readiness Team Database; and provides corrective actions for all identified incidents.

Audit Logs. Audit logs are a key component to computer security architecture and network security. An audit log is a sequential record of all actions performed on a device. Security personnel use audit logs to identify current and past device activity as well as names of individuals or systems conducting activity. For instance, when a computer performs a request (data search, website access, e-mail "send"), the network equipment involved (router, firewall, website server) records an audit log entry of each action. These logs preserve data for future analysis to determine technical or operational impacts of detected events. Maintaining audit logs is vital to finding the true source network address that introduced harmful activities into the Air Force network. Air Force Records Information Managements System, Series 33 table 25 rule 8, 3 June 2005, requires automated or manual records (audit trials) that identify automated information system access attempts (pass or fail) be retained for at least one year.

Categorizing Events. Once the "true source" is identified, AFCERT personnel categorize the event 1 through 9 based on severity ranking criteria listed in Air Force Instruction (AFI) 33-138, *Enterprise Network Operations Notification and Tracking,* 28 November 2005. For example, a category 5 event is activity that may expose Air Force systems to increased risk due to authorized or unauthorized user actions. This could include an Air Force network administrator not applying a computer update or an internal user

[1] Air National Guard Network Operations and Security Center, 83d Integrated Network Operation and Security Center and 561st Integrated Network Operation and Security Center.

[2] A network firewall protects a computer from unauthorized access by controlling network data flow.

[3] A proxy server acts as a firewall by receiving and selectively blocking data flow.

[4] The domain name server assists the network by automatically converting a network name or web address to a numerical Internet Protocol (IP) address.

introducing a virus to the network. Investigating events is critical in determining whether an event should be designated an incident requiring corrective action.

Cyber Warfare policy. The Cyberspace Operations Network Warfare Division (AF/A3Z-CW) must develop cyber warfare policy to include network attack, defense and warfare support.

AUDIT RESULTS 1 - INVESTIGATION

Condition. Network personnel did not investigate cyber events. Specifically, network personnel at all three I-NOSCs did not investigate 18 (23 percent) of 78 category 5 cyber events[5] reviewed. For example, network personnel did not investigate an IP address[6] at Seymour Johnson AFB attempting to access a domain known to host malicious files.

Cause. This condition occurred because network personnel did not retain proxy server, firewall and DSN audit logs needed to identify "true source." Specifically, none of the three I-NOSCs reviewed retained audit logs for the required one year (Table 1). To illustrate, of the 25 installations reviewed:

- Proxy Server Logs. Twenty-four (96 percent) did not retain proxy server logs for one year. For example, network personnel at Maxwell AFB retained proxy logs for only 20 days.

- Firewall Logs. Twenty-four (96 percent) did not retain firewall logs for one year. For example, network personnel at Charleston AFB retained firewall logs for only 21 days. The ANG network personnel could not provide retention firewall timeframes at eight (100 percent) installations because each wing and detachment individually retains their logs.

- DNS Logs. Seventeen (68 percent) did not retain DNS logs for one year. For example, all eight (100 percent) installations under the 561st I-NOSC did not retain any DNS audit logs and five (56 percent) installations within the 83d I-NOSC retained their logs for less than 7 days.

[5] Selected from a universe of 407 category five events.

[6] A number used by a computer to send and receive network data.

I-NOSC	Installations	Proxy Log Retention (Days)	Firewall Log Retention (Days)	DNS Log Retention (Days)
ANG	Abraham Lincoln Capital Airport (Arpt)	60	Unknown	456
ANG	Allen C Thompson Field	60	Unknown	459
561st	Altus AFB	20	50	0
ANG	Birmingham Arpt	60	Unknown	455
83d	Brooks City-Base	41	58	7
83d	Dobbins Air Reserve Base (ARB)	92	90	70
561st	Eielson AFB	84	443	0
83d	Ellsworth AFB	83	50	32
ANG	Forbes Field	60	Unknown	460
83d	Grissom ARB	92	90	32
83d	Hanscom AFB	82	40	6
83d	Joint Base (JB) Andrews	62	40	6
561st	JB Charleston	237	21	0
ANG	Klamath Falls Arpt	60	Unknown	459
561st	Kunsan Air Base (AB)	360	28	0
561st	Los Angeles AFB	326	350	0
561st	Maxwell AFB	20	50	0
83d	Moron AB	21	89	1-2
561st	McConnell AFB	367	51	0
ANG	McGhee Tyson Arpt	60	Unknown	449
ANG	Naval Air Station (NAS) Joint Reserve Base (JRB) New Orleans	60	Unknown	458
83d	Nellis AFB	212	38	33
561st	Patrick AFB	326	328	0
ANG	Pease International Tradeport ANG Station	60	Unknown	458
83d	Ramstein AB	92	39	1-2

Table 1. Audit Logs

Installation NCC personnel did not retain audit logs because they did not have the computer data storage capacity needed to retain multiple logs for one year. Additionally, the Director, Operations, Plans, and Requirements Cyberspace Operations Network Warfare Division (AF/A3/5/A3Z-CW) did not establish I-NOSC-specific audit log retention policy. As a result, each I-NOSC developed their own storage policy ranging from zero to 90 days.

Effect. Cyber event investigations are crucial for responding to and preventing future network attacks. Maintaining proxy server, firewall and DNS audit logs provides the critical information needed to determine the "true source" of an event and begin mitigating response actions. Without audit log retention and review, an infected computer may reside on the Air Force network undetected.

Recommendation A.1. The Air Force Space Command Commander (AFSPC/CC) should direct the 24th Air Force Commander acquire sufficient storage capacity for the I-NOSCs to retain audit logs in accordance with the Air Force Records Information System Disposition Schedule.

Management Comments A.1. The AFSPC/A3 concurred and stated: "Our Cyberspace program office at Electronic Systems Center is working on a Tech Refresh for storage; this includes base boundary ($25 million) and both I-NOSCs ($59 million). The AFSPC will establish requirements for which system audit logs are required to support sources and methods intelligence for 5 years and which only have a 1-year retention. The AFSPC will establish minimum interim requirements for audit logs until program actions can fund the full requirement. The ANG/A6 purchase includes standardized server virtualization, storage, and backup capabilities for all 102 NCCs, 6 Regional Centers and Area Processing Centers. The ANG installed the solution at six pilot sites and has begun rollout to remaining sites at the time of this report. This infrastructure reconstruction completely changes the capabilities currently in place. The new backup solution rolled out under this project provides for data de-duplication to enable more data saved on less disk space. Estimated Completion Date: 1 January 2012. (A full text of AFSPC/A3 management comments is at Appendix II)."

Recommendation A.2. The AF/A3/5 should direct AF/A3Z-CW revise Air Force guidance to require I-NOSCs retain audit logs in accordance with the Air Force Records Information System Disposition Schedule.

Management Comments A.2. The AF/A3/5 concurred and stated: "The AF/A3/5 has directed the AF/A3Z-CW to develop AFI 10-1702, *Network Incident Handling*, which will contain minimum requirements in assisting with response to cyber events/incidents to include log retention criteria. The AFI 10-1702 will not be published until AFPD 10-17, *Cyberspace Operations* is published in accordance with AFI 33-360. Estimated Completion Date: 1 January 2012."

Evaluation of Management Comments. Management comments addressed the issues raised in the audit results, and management actions taken or planned should correct the problem.

Tab B
Corrective Actions

BACKGROUND

Server Configuration. The Air Force Network Operations Center (AFNOC) issued Network Operations Tasking Order (NTO) 2007-311-003A, 7 November 2007, requiring SmartFilters be used on all Air Force proxy servers to standardize web content filtering and restrict access to selected website categories. On 28 January 2008, I-NOSC West issued Maintenance Tasking Order (MTO) 2008-024-006B, to transition the Air Force from using SmartFilter to Blue Coat Webfilters™ software on proxy servers. This MTO established a proxy server web content filtering standard for all I-NOSCs.

AUDIT RESULTS 2 – CORRECTIVE ACTIONS

Condition. Network personnel did not implement corrective actions to prevent cyber incidents from recurring. Specifically, network personnel at all three I-NOSCs did not comply with MTO 2008-024-006B to properly configure Blue Coat Web Filters on proxy servers to restrict access to the following unauthorized website categories: greeting cards, software downloads, alcohol, auctions, unwanted software, television video streams, media sharing, pay-to-surf, radio streams, social networking, streaming media and open image/media. For example, I-NOSC West personnel, who manage proxy servers for 28 AFSPC installations and 57 non-AFSPC installations, did not configure Blue Coat Webfilters™ to restrict the "greeting cards," "unwanted software" or "software download" categories on all 85 proxy servers under their operational control.

Cause. This condition occurred because AF/A3Z-CW did not establish a standard list of restricted proxy server categories. Therefore, the MTO created confusion as to which categories (former SmartFilter or Blue Coat Filter categories) to restrict. For example, greeting card is a restricted Blue Coat Webfilters™ category, but not a restricted SmartFilter category. Consequently, I-NOSC personnel used their own judgment when choosing categories to restrict.

Effect. Implementing cyber incident corrective actions improves Air Force defense in-depth strategy to ensure networks are available to warfighters and reduces network vulnerability to malicious activity intent on degrading and disrupting network operation. Accurately configuring proxy server settings is essential for mitigating threats to the Air Force network. For example, 22 (28 percent) of 78 category five security incidents reviewed could have been minimized or prevented had proxy servers been properly configured.

Recommendation B.1. The AF/A3/5 should direct AF/A3Z-CW personnel revise Air Force guidance to establish a standard list of restricted proxy server categories.

Management Comments B.1. The AF/A3/5 concurred and stated: "The AF/A3/5 has directed the 624 Operations Center (OC) to de-conflict the restriction categories. Estimated Completion Date: 1 January 2012."

Recommendation B.2. The AFSPC/CC should direct the 24 AF/CC require I-NOSCs configure proxy servers to comply with AF/A3Z-CW standard list of restricted proxy server categories.

Management Comments B.2. The AFSPC/A3 concurred and stated: "All base fire-walls should have a standard set of blocked sites and services. The AF/A3Z-C (formerly AF/A30-CON) should publish a standard list of restricted proxy server categories. The 24 AF/CC will require I-NOSCs configure proxy servers to comply with the 624th OC de-conflicted restriction categories. Estimated Completion Date: 1 January 2012. (A full text of AFSPC/A3 management comments is at Appendix II)."

Evaluation of Management Comments. Management comments addressed the issues raised in the audit results, and management actions planned should correct the problem.

Incident Response and Reporting. The purpose of incident detection, investigation, vulnerability correction, and the subsequent report process is to improve the Air Force Enterprise Network's (AFEN) overall security. The AFCERT monitors traffic on the Air Force network, and when a suspicious activity is identified, the activity is classified as an "event." Each event is investigated, and if determined to be a security breach, designated as an "incident." The AFEN incidents (hereafter identified as security incidents) include root-level intrusion, user-level intrusion, denial of service, or malicious logic. A security incident may also involve a violation of law.

Intrusion Detection. The Air Force primary intrusion detection tool is the fleet of Automated Security Incident Measurement Sensors (ASIMS) deployed across the AFEN. The ASIMS *Installation and User's Guide,* December 2003, describes the ASIMS as a mission-critical tool that supports computer network defense operations. It operates in real time as it collects network traffic and identifies strings and services[7] that could indicate cyber incidents. Attempts against Air Force network called incidents include attempted entry, unauthorized entry, and attacks on an information system to include: unauthorized probing, browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to system hardware, firmware, or software characteristics with or without the users knowledge. Table 2 below defines the nine categories the Air Force uses to characterize detected events and incidents.

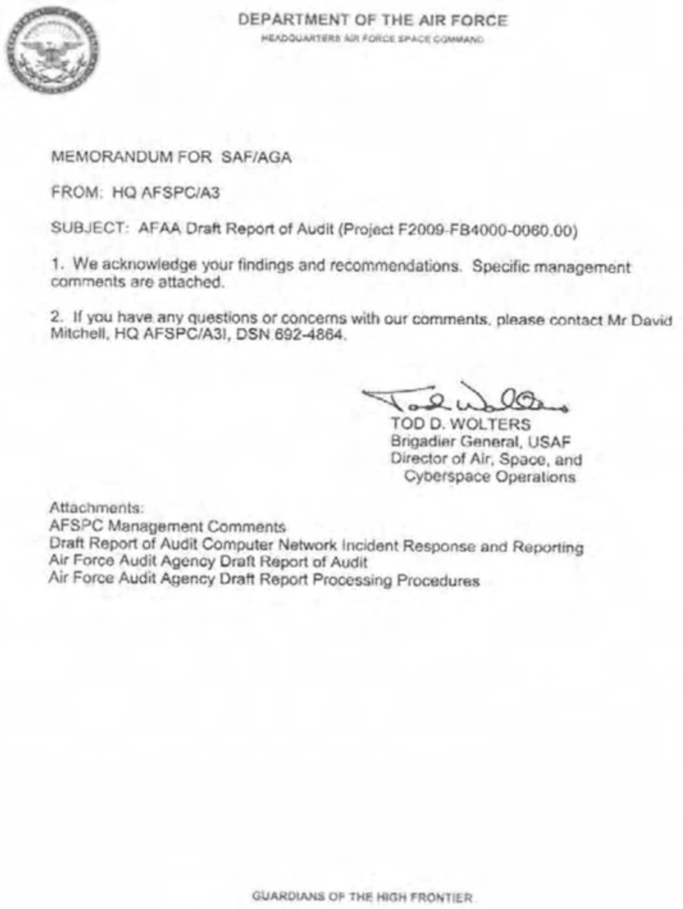
Category	Description
I	**Root Level Intrusion (Incident)** – An unauthorized person gained root-level access/privileges on an Air Force computer/information system/network device.
II	**User Level Intrusion (Incident)** – An unauthorized person gained user-level privileges on an Air Force computer/information system/network device.
III	**Unsuccessful Activity Attempt (Event)** - An unauthorized person specifically targeted a service/vulnerability on an Air Force computer/information system/network device in an attempt to gain unauthorized or increased access/privileges, but was denied access.
IV	**Denial of Service (DoS) (Incident)** – Air Force computer/information system/network use was denied due to an overwhelming volume of unauthorized network traffic.
V	**Non-Compliance Activity (Event)** – An Air Force computer/information system/network was incorrectly configured or a user did not follow established policy.
VI	**Reconnaissance (Event)** – Active ports on an Air Force computer/information system/network device was scanned with no DoS or mission impact.
VII	**Malicious Logic (Incident)** – Hostile code successfully infected an Air Force computer/information system/network device.
VIII	**Investigating (Event)** – Air Force network events that are potentially malicious or anomalous activity deemed suspicious and warrant, or are undergoing further review.
IX	**Explained Anomaly (Event)** – Air Force network suspicious events that after further investigation are determined to be nonmalicious activity and do not fit the criteria for any other categories.

Table 2. Incident and Event Categories

[7] Strings are specific sequences of bytes (often called attack signatures) that are known to appear in the malicious traffic.

This Page Intentionally Left Blank

"TRUE COPY"



DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE SPACE COMMAND

MEMORANDUM FOR SAF/AGA

FROM: HQ AFSPC/A3

SUBJECT: AFAA Draft Report of Audit (Project F2009-FB4000-0060.00)

1. We acknowledge your findings and recommendations. Specific management comments are attached.

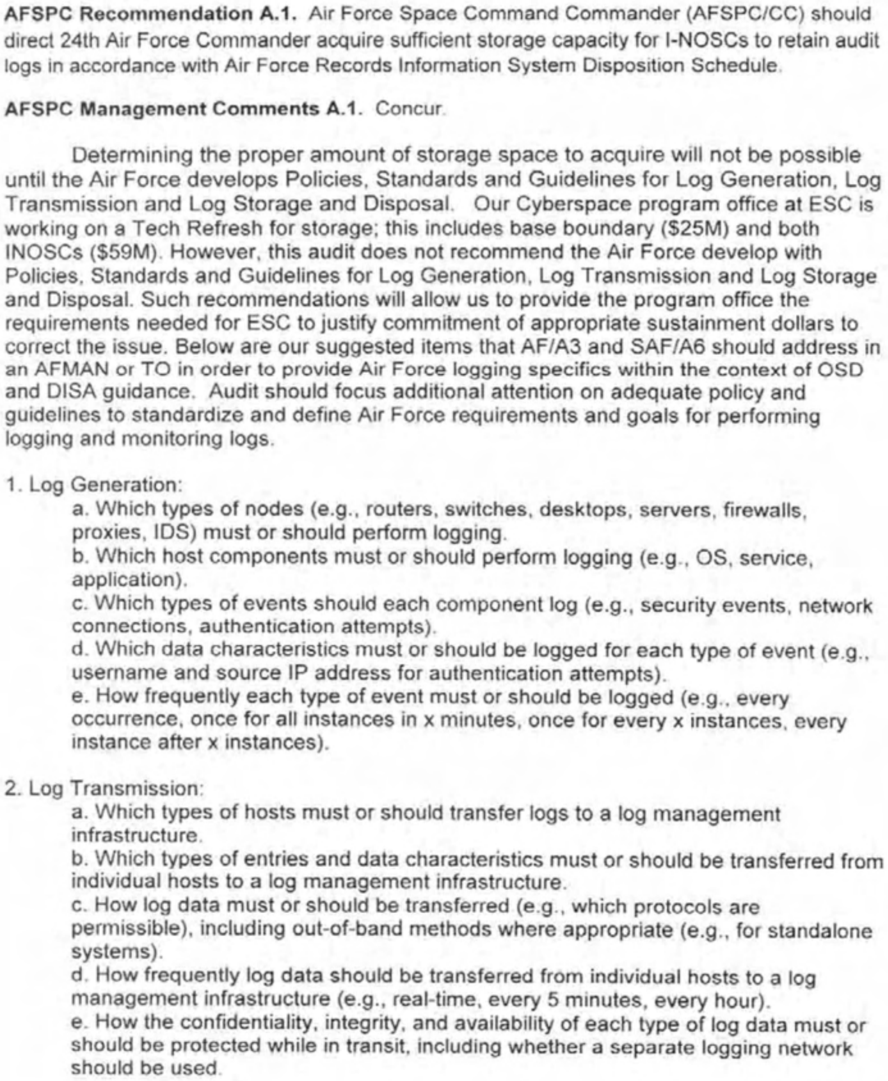
2. If you have any questions or concerns with our comments, please contact Mr David Mitchell, HQ AFSPC/A3I, DSN 692-4864.

TOD D. WOLTERS
Brigadier General, USAF
Director of Air, Space, and
Cyberspace Operations

Attachments:
AFSPC Management Comments
Draft Report of Audit Computer Network Incident Response and Reporting
Air Force Audit Agency Draft Report of Audit
Air Force Audit Agency Draft Report Processing Procedures

GUARDIANS OF THE HIGH FRONTIER

"TRUE COPY"



AFSPC Recommendation A.1. Air Force Space Command Commander (AFSPC/CC) should direct 24th Air Force Commander acquire sufficient storage capacity for I-NOSCs to retain audit logs in accordance with Air Force Records Information System Disposition Schedule.

AFSPC Management Comments A.1. Concur.

Determining the proper amount of storage space to acquire will not be possible until the Air Force develops Policies, Standards and Guidelines for Log Generation, Log Transmission and Log Storage and Disposal. Our Cyberspace program office at ESC is working on a Tech Refresh for storage; this includes base boundary ($25M) and both INOSCs ($59M). However, this audit does not recommend the Air Force develop with Policies, Standards and Guidelines for Log Generation, Log Transmission and Log Storage and Disposal. Such recommendations will allow us to provide the program office the requirements needed for ESC to justify commitment of appropriate sustainment dollars to correct the issue. Below are our suggested items that AF/A3 and SAF/A6 should address in an AFMAN or TO in order to provide Air Force logging specifics within the context of OSD and DISA guidance. Audit should focus additional attention on adequate policy and guidelines to standardize and define Air Force requirements and goals for performing logging and monitoring logs.

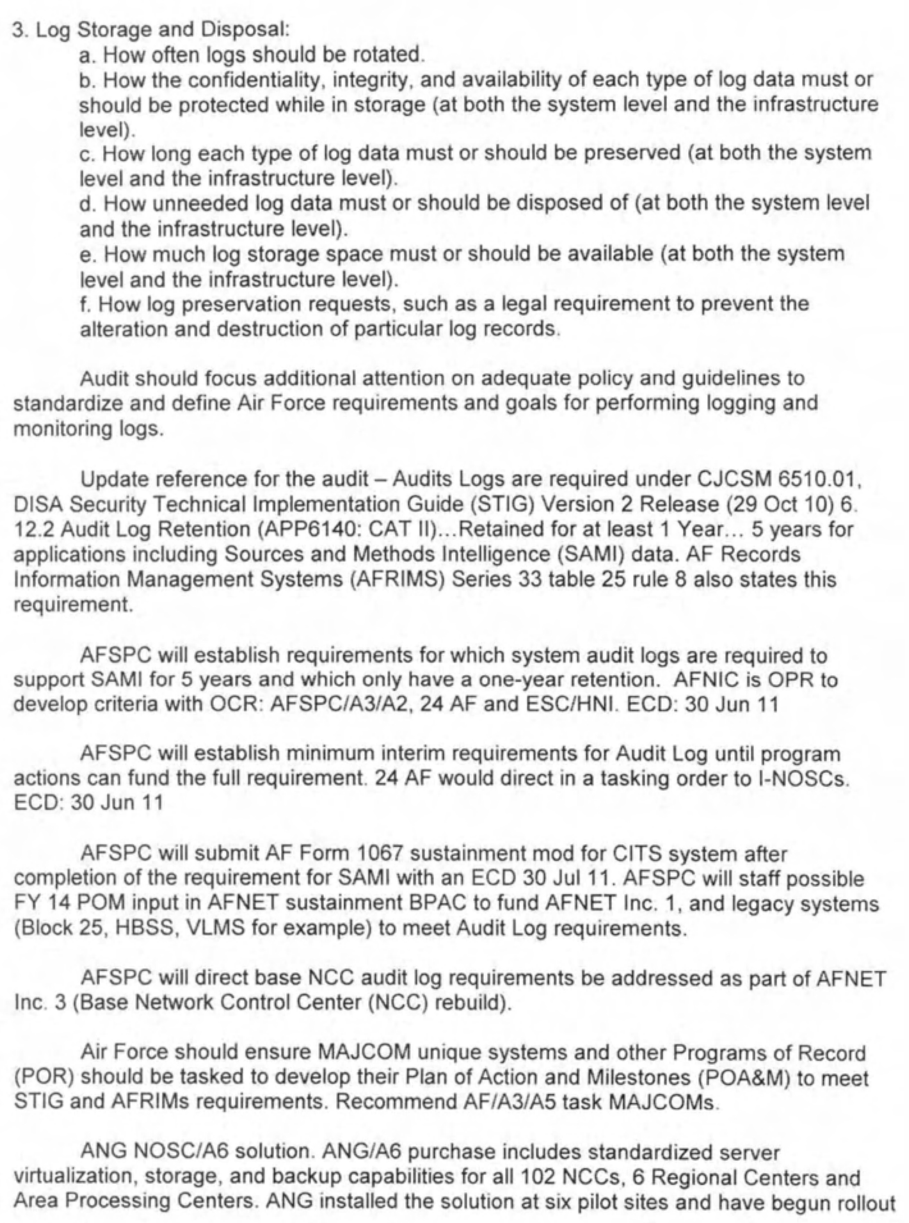
1. Log Generation:

a. Which types of nodes (e.g., routers, switches, desktops, servers, firewalls, proxies, IDS) must or should perform logging.
b. Which host components must or should perform logging (e.g., OS, service, application).
c. Which types of events should each component log (e.g., security events, network connections, authentication attempts).
d. Which data characteristics must or should be logged for each type of event (e.g., username and source IP address for authentication attempts).
e. How frequently each type of event must or should be logged (e.g., every occurrence, once for all instances in x minutes, once for every x instances, every instance after x instances).

2. Log Transmission:

a. Which types of hosts must or should transfer logs to a log management infrastructure.
b. Which types of entries and data characteristics must or should be transferred from individual hosts to a log management infrastructure.
c. How log data must or should be transferred (e.g., which protocols are permissible), including out-of-band methods where appropriate (e.g., for standalone systems).
d. How frequently log data should be transferred from individual hosts to a log management infrastructure (e.g., real-time, every 5 minutes, every hour).
e. How the confidentiality, integrity, and availability of each type of log data must or should be protected while in transit, including whether a separate logging network should be used.

"TRUE COPY"



3. Log Storage and Disposal:
   - a. How often logs should be rotated.
   - b. How the confidentiality, integrity, and availability of each type of log data must or should be protected while in storage (at both the system level and the infrastructure level).
   - c. How long each type of log data must or should be preserved (at both the system level and the infrastructure level).
   - d. How unneeded log data must or should be disposed of (at both the system level and the infrastructure level).
   - e. How much log storage space must or should be available (at both the system level and the infrastructure level).
   - f. How log preservation requests, such as a legal requirement to prevent the alteration and destruction of particular log records.

Audit should focus additional attention on adequate policy and guidelines to standardize and define Air Force requirements and goals for performing logging and monitoring logs.

Update reference for the audit – Audits Logs are required under CJCSM 6510.01, DISA Security Technical Implementation Guide (STIG) Version 2 Release (29 Oct 10) 6. 12.2 Audit Log Retention (APP6140: CAT II)...Retained for at least 1 Year... 5 years for applications including Sources and Methods Intelligence (SAMI) data. AF Records Information Management Systems (AFRIMS) Series 33 table 25 rule 8 also states this requirement.

AFSPC will establish requirements for which system audit logs are required to support SAMI for 5 years and which only have a one-year retention. AFNIC is OPR to develop criteria with OCR: AFSPC/A3/A2, 24 AF and ESC/HNI. ECD: 30 Jun 11

AFSPC will establish minimum interim requirements for Audit Log until program actions can fund the full requirement. 24 AF would direct in a tasking order to I-NOSCs. ECD: 30 Jun 11

AFSPC will submit AF Form 1067 sustainment mod for CITS system after completion of the requirement for SAMI with an ECD 30 Jul 11. AFSPC will staff possible FY 14 POM input in AFNET sustainment BPAC to fund AFNET Inc. 1, and legacy systems (Block 25, HBSS, VLMS for example) to meet Audit Log requirements.

AFSPC will direct base NCC audit log requirements be addressed as part of AFNET Inc. 3 (Base Network Control Center (NCC) rebuild).

Air Force should ensure MAJCOM unique systems and other Programs of Record (POR) should be tasked to develop their Plan of Action and Milestones (POA&M) to meet STIG and AFRIMs requirements. Recommend AF/A3/A5 task MAJCOMs.

ANG NOSC/A6 solution. ANG/A6 purchase includes standardized server virtualization, storage, and backup capabilities for all 102 NCCs, 6 Regional Centers and Area Processing Centers. ANG installed the solution at six pilot sites and have begun rollout

"TRUE COPY"

to remaining sites at the time of this report. This infrastructure re-construction completely changes the capabilities currently in place. The new backup solution rolled out under this project provides for data de-duplication to enable more data saved on less disk space. However, it is not confirmed if there is enough storage for all backup timelines. ANG will have a better idea on their capabilities by late summer 2011. Better Air Force guidance will help determine specific storage requirement gaps. Project schedule for full implementation is August 2012.

We do not envision any potential monetary benefits, we expect over $100M in additional costs for storage.

Overall ECD: 1 January 2012, but realistically complete implementation could take a number of years.

AFSPC Recommendation B.2. AFSPC/CC should direct 24 AF/CC require I-NOSCs configure proxy servers to comply with AF/A3Z-CW standard list of restricted proxy server categories.

AFSPC Management Comments B.2. Concur.

All base firewalls should have a standard set of blocked sites and services. AF/A3Z-C (formerly AF/A3O-CON) should publish a standard list of restricted proxy server categories. The 24 AF/CC will require I-NOSCs configure proxy servers to comply with the 624 Operations Center de-conflicted restriction categories. ECD: 1 January 2012, but realistically all actions would be completed within a few weeks after AF/A3Z-C provides a published list of restricted proxy server categories.

AUDIT SCOPE

Audit Coverage. We performed the audit at three judgmentally selected I-NOSCs and the AFCERT (Appendix IV). We held discussions with the Chief, Warfighting Integration and Chief Information Officer Information Assurance Division (SAF/CIO A6NI), AFCERT, AF/A3Z-CW personnel and AFSPC NOSC Commanders, including 561st and 83d NOS Commanders. We performed the audit from January 2010 through May 2010 using documents dated from 29 January 2007 to 22 April 2010. We provided a draft report to management in December 2010.

- Criteria/Methodology. We obtained and reviewed the AFI 33-138, Air Force MTOs and NTOs, and AFRIMS. We also met with AFCERT personnel to discuss policies on how cyber events and incidents are determined and reported.

- Proxy Server Logs. To determine whether I-NOSC personnel retained proxy server logs required to investigate cyber events, we obtained and reviewed audit logs for proxy servers at 25 locations within the three I-NOSCs. We interviewed the administrators and obtained computer screen shots for evidence of log retention and verified online and offline log retention periods. Further, we reviewed a sample of category five events to determine the number of events closed due to inability to determine the true source.

- Firewall Logs. To determine whether I-NOSC personnel retained firewall logs required to investigate cyber events, we obtained and reviewed audit logs for firewalls at 25 locations within the three I-NOSCs. We interviewed the administrators and obtained computer screen shots for evidence of log retention and verified online and offline log retention periods. Further, we reviewed a sample of category five events to determine the number of events closed due to inability to determine true source.

- DNS Logs. To determine whether I-NOSC personnel retained DNS logs required to investigate cyber events, we obtained and reviewed audit logs for DNS at 25 locations within the three I-NOSCs. We interviewed the administrators and obtained computer screen shots for evidence of log retention and verified online and offline log retention periods. Further, we reviewed a sample of category five events to determine the number of events closed due to inability to determine true source.

- Blue Coat Webfilters™. To determine whether I-NOSC personnel identified and implemented corrective actions by configuring blue coat proxy servers to comply with MTO 2008-024-006B, 28 January 2008, we interviewed the administrators and obtained computer screen shots of the central and local policies in the blue coat director web interface at each I-NOSC. We discussed review and update procedures, verified online configuration settings by obtaining available screen shots, and obtained evidence of management oversight for proxy server configurations.

Sampling Methodology. We used the following sampling concepts and computer-assisted auditing tools and techniques (CAATTs) to complete this audit.

- Sampling. We used judgmental and random sampling to accomplish the audit. Specifically, we judgmentally selected 25 locations within the three I-NOSCs with more than ten incidents in calendar year 2009 to review. We reviewed 100 percent of the incidents at locations with less than 30 incidents and randomly selected 30 incidents for those locations with more than 30 incidents.

- CAATTs. We used CAATTs extensively throughout this audit. Specifically, we used advanced Excel® spreadsheet features and functions (COUNTIF) to quickly summarize audit data used to develop audit conclusions.

Data Reliability. We relied on computer-processed data contained in the Joint Computer Emergency Readiness Team and Remedy Databases. We did not evaluate the general and application controls for the Joint Computer Emergency Readiness Team or Remedy Databases. However, to establish data reliability, we compared output data to manual documents to validate data accuracy; reviewed output products for obvious errors, reasonableness and completeness. Based on these tests, we concluded that the data were reliable to support audit conclusions.

Auditing Standards. We conducted this performance audit in accordance with 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 the audit objectives. We believe the evidence obtained provides a reasonable basis for the findings and conclusions cited in this report.

Internal Controls. We reviewed internal controls to determine whether the Air Force effectively managed cyber events and incidents. Specifically, we reviewed (a) incident report records, (b) proxy server, firewall and DNS audit log review and retention, (c) proxy server configurations, and (d) incident response training.

PRIOR AUDIT COVERAGE

We did not identify any Air Force Audit Agency, DoD Inspector General, or Government Accountability Office reports issued within the past 5 years that addressed the same or similar objectives as this audit.

Locations Audited/ Reports Issued

Organization/Location	Installation-Level Reports Issued
HQ Air Combat Command	
83d Integrated Network Operations and Security Center Joint Base Langley VA	F2010-0054-FDM000 20 July 2010
HQ Air Force Space Command	
561st Integrated Network Operations and Security Center Peterson AFB CO	F2011-0016-FBM000 3 December 2010
33d Network Warfare Squadron Air Force Computer Emergency Response Team Lackland AFB TX	None
Air National Guard	
Air National Guard Network Operations and Security Center McConnell AFB KS	F2010-0055-FBL000 17 June 2010

This Page Intentionally Left Blank

Points of Contact

Cyber Security Assurance Division (AFAA/FSS)
Financial and Systems Audits Directorate
5023 4th Street
March ARB CA 92518-1852

Bruce Carpenter, Associate Director
DSN 447-4929
Commercial (951) 655-4929

[redacted], Program Manager

[redacted], Audit Manager

We accomplished this audit under project number F2009-FB4000-0060.000.

This Page Intentionally Left Blank

Final Report Distribution

SAF/OS
SAF/US
SAF/FM
SAF/IG
SAF/LL
SAF/PA
SAF/XC, AF/A6
AF/CC
AF/CV
AF/CVA
AF/A8
AF/RE

AU Library
DoD Comptroller
OMB

ACC
AETC
AFGSC
AFISR
AFMA
AFMC
AFOSI
AFRC
AFSOC
AFSPC
AMC
ANG
PACAF
USAFA
USAFE
Units/Orgs Audited

FREEDOM OF INFORMATION ACT

The disclosure/denial authority prescribed in AFPD 65-3 will make all decisions relative to the release of this report to the public.

This Page Intentionally Left Blank

To request copies of this report or to suggest audit topics for future audits, contact the Operations Directorate at (703) 696-8088 (DSN 426-8088) or E-mail to reports@pentagon.af.mil. Certain government users may download copies of audit reports from our Air Force Knowledge Now page at https://afkm.wpafb.af.mil/ASPs/CoP/OpenCoP.asp?Filter=OO-AD-01-41. Finally, you may mail requests to:

Air Force Audit Agency
Operations Directorate
1126 Air Force Pentagon
Washington DC 20330-1126