AIR FORCE AUDIT AGENCY

NATIONAL SECURITY SYSTEM CLASSIFICATION

AUDIT REPORT

F2012-0001-FB2000

18 November 2011

Executive Summary

INTRODUCTION

The Office of the Secretary of the Air Force, Chief Information Officer (SAF/CIO A6) is the office of primary responsibility for National Security Systems (NSSs). As of 4 November 2010, management uses the Enterprise Information Technology Data Repository (EITDR) to retain oversight of the Air Force's 422 NSSs.

OBJECTIVES

We performed this audit due to the sensitive nature of the national security systems. The objective of this audit was to determine whether Air Force personnel properly classified Information Technology (IT) systems as national security systems. Specifically, we determined whether IT systems currently not classified as NSS should have been classified as NSS.

CONCLUSIONS

Air Force program management personnel did not always properly classify IT systems with regards to NSS. Specifically, Air Force personnel did not properly classify one individual system and two groups of systems, potentially over classifying their status as an NSS. As a result, information systems incorrectly classified as NSS are not scrutinized and reviewed for compliance in the same manner as systems associated with business mission area. Both the Chief Information Officer and Chief Management Officer have Congressional mandates to review all business mission area IT systems as a major capital investment for the life cycle of the system as well as monitor them for performance, costs, and capabilities. (Tab A, page 1)

RECOMMENDATIONS

We made one recommendation to improve NSS classification. (Reference Tab A for the specific recommendation).

MANAGEMENT'S RESPONSE

Management concurred with the findings and recommendations contained in this report. Accordingly, this report contains no issues requiring elevation for resolution.

[redacted]

Program Manager
(Information Systems Development Division)

Alfred J. Massey

ALFRED J. MASSEY
Acting Assistant Auditor General
(Financial and Systems Audits)

Table of Contents

BACKGROUND

The National Institute of Standards and Technology (NIST) developed a National Security Checklist[1] that establishes criteria to classify information systems as NSS. The SAF/CIO A6P incorporated the criteria into the EITDR so that program managers and information technology portfolio managers can identify an information system as NSS when applicable. (See Appendix I for more detailed explanation of the NIST criteria and the NSS classification process flow.)

The NSS classification is applicable to all IT systems[2] and initiatives.[3] Also, the NSS applies to all IT portfolio mission areas (Business Mission Area, Warfighting Mission Area, and potentially the Enterprise Information Environment (EIE) Mission Area). While the Business and Warfighting mission areas are indicative of their names, the EIE mission area represents the common, integrated information computing and communications environment. The EIE mission area is composed of assets that operate as, provide transport for, and/or assure local area networks computing capabilities.

The EIE's primary emphasis pertains to infrastructure to include hardware, software operating systems, and hardware/software support that enable the Global Information Grid (GIG) enterprise. This includes both non-classified and secure networks. To illustrate, an example of infrastructure is the Secret Internet Protocol Router Network (SIPRNet), a wide area network that is separated both physically and logically from other networks. Another infrastructure, video teleconferencing (VTC), supports desktop computers, video, cable television, and video teleconference briefings. Video teleconferencing can be "point-to-point" between two sites or between multiple points.

AUDIT RESULTS 1 – CLASSIFICATION

Condition. Air Force program management personnel did not properly classify all IT systems. Specifically, Air Force personnel did not properly classify one individual system and two groups of systems, potentially over classifying their status as an NSS. Specifically:

[1] Guideline for Identifying an Information System as a National Security System (NSS), August 2003. This guideline provides six basic criteria to identify an information system as a NSS.

[2] A system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.

[3] Denotes a collection of resources that are focused on a single IT project. These initiatives include both new starts and ongoing efforts.

- System. Program personnel incorrectly classified the T38 Integrated Maintenance Information System as NSS. This is an aircraft maintenance system and should not be classified as NSS.

- Groups. Program personnel incorrectly classified scenarios involving groups of systems and enclaves as NSS. To illustrate,

    - The Air Force Weather Agency (AFWA) personnel submitted a request to SAF/A6P classifying an enclave[4] of 30 weather systems as NSS without initially assessing each information system individually against the NIST criteria. In addition, SAF/A6P agreed the enclave was NSS. For example, two weather collection systems were potentially over classified and do not qualify as NSS:

        - Tactical Meteorological Observing Set performs routine weather data gathering (wind speed, humidity, temperature, and dew points).

        - Next Generation Ionosonde, an unmanned ionosonde facility, senses and reports ionospheric information for comprehensive and ongoing environmental analysis.

    - Air Force IT program management personnel inconsistently classified EIE Mission Area infrastructure (SIPRNet circuit enclaves and VTCs) as NSS without accurately assessing them against the NIST criteria. To illustrate:

        - Ninety-seven of 243 (40 percent) SIPRNet circuit enclaves were classified as NSS even though SIPRNet is an information transportation infrastructure. Meanwhile the remaining 60 percent were not.

        - Nine of 98 (9 percent) video teleconferencing systems were classified as NSS even though VTCs are infrastructures to include hardware and software that assist in the passing of information from point-to-point.

Cause. These discrepancies occurred for two reasons.

- Management determined there was a relationship between aircraft maintenance and sustainability. This determination caused the program manager to classify the system as NSS criteria.

[4] Enclave donates a collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function independent of location.

- While SAF/A6P provided guidance for classifying systems as NSS, they did not explain to program managers and IT portfolio manager's effective methods to evaluate scenarios involving enclaves and infrastructures as NSS. Specifically, SAF/A6P did not establish a method to evaluate:

  - Enclaves of systems without first assessing each system individually to ensure those that do not meet the intent of the NIST criteria are not classified as NSS.

  - EIE mission area systems, specifically infrastructure (SIPRNet circuit enclaves and VTCs) as NSS.

Effect. As a result, information systems misclassified as NSS are not scrutinized and reviewed for compliance in the same manner as systems associated with business mission area. Both the Chief Information Officer and Chief Management Officer have Congressional mandates to review all business mission area IT systems as a major capital investment for the life cycle of the system as well as monitored them for performance, costs, and capabilities.

Audit Comment. Management submitted a request to correct the classification of the T38 Integrated Maintenance Information System; therefore, no recommendation is made regarding this one system.

Recommendation A.1. The Secretary of the Air Force Chief Information Officer should provide guidance to the field related to unique groups of systems involving enclaves and infrastructure by**:**

a. Evaluating any enclave of systems and individually assess each system against the NSS criteria. After assessed, each system should be adjusted accordingly.

b. Approving enclave requests only when they have had the program managers demonstrate each system was individually assessed against the NSS criteria.

c. Establishing a method to identify if and when EIE Mission Area systems, specifically infrastructure (SIPRNet circuit enclaves and VTCs), should be considered as NSS.

Management Comments A.1. SAF/A6P concurred and stated:

a. "Each system in an enclave will be individually reviewed against the NSS criteria to ensure proper categorization regardless of what enclave the system will be hosted in. However, all SIPRNet enclaves must be categorized as NSS based on criteria outlined in Federal Information Security Management Act (FISMA) and guidance provided in National Institute of Standards and Technology, Special Publication (NIST SP) 800-59. Estimated Completed Date: 31 December 2011.

a. “The NSS categorization process will be defined to ensure only representatives from the Air Force Chief Information Officer (CIO) or Air Force Senior Information Assurance Officer (SIAO) can validate proper NSS categorization. The proposed process will be codified into Air Force policy (Air Force Instruction 33-141). Estimated Completion Date: 30 April 2012.

b. “The SAF/A6OI in conjunction with SAF/A6PP (EITDR data support) will review all systems currently registered in EITDR for proper NSS categorization. Estimated Completion Date: 30 November 2011.”

Evaluation of Management Comments. Management concurred with the audit results, and corrective actions planned should correct the problems identified.

The NIST developed a National Security Checklist that establishes criteria to classify information systems as NSS. For a system to be classified as a NSS, it must be involved in one of these six areas: 1) intelligence activities; 2) cryptologic activities related to national security; 3) command and control of military forces; 4) equipment that is integral part of a weapon(s) system; 5) is critical to the fulfillment of military or intelligence missions; or 6) is protected by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense of foreign policy.

The SAF/CIO A6P, developed a "*Proposed Operational Support Business System NSS Classification Process*, 8 February 2007." This document provides program management personnel, IT portfolio managers, and Chief Information Officers the process and steps they need to accomplish when classifying a system as a NSS. The process includes a flowchart called "*Air Force Operational Support Business System NSS Classification Review/Approval Process*" (Exhibit 1).

This flowchart outlines the NSS approval process from the program manager to portfolio manager up through the functional Chief Information Officer and Certification Process Manager. EITDR includes the guidance that helps program management determine whether the system is NSS.

The EITDR lists all Air Force systems, initiatives, and infrastructures (SIPRNet circuit enclaves and VTC). These information transportation infrastructures provide a means to transmit data from one point to another by the use of network circuits.

Also, these systems are identified in EITDR by the business mission area, Enterprise Information Environment. This designation means the assets operate as, provide transport for, or assure local area networks computing capabilities.

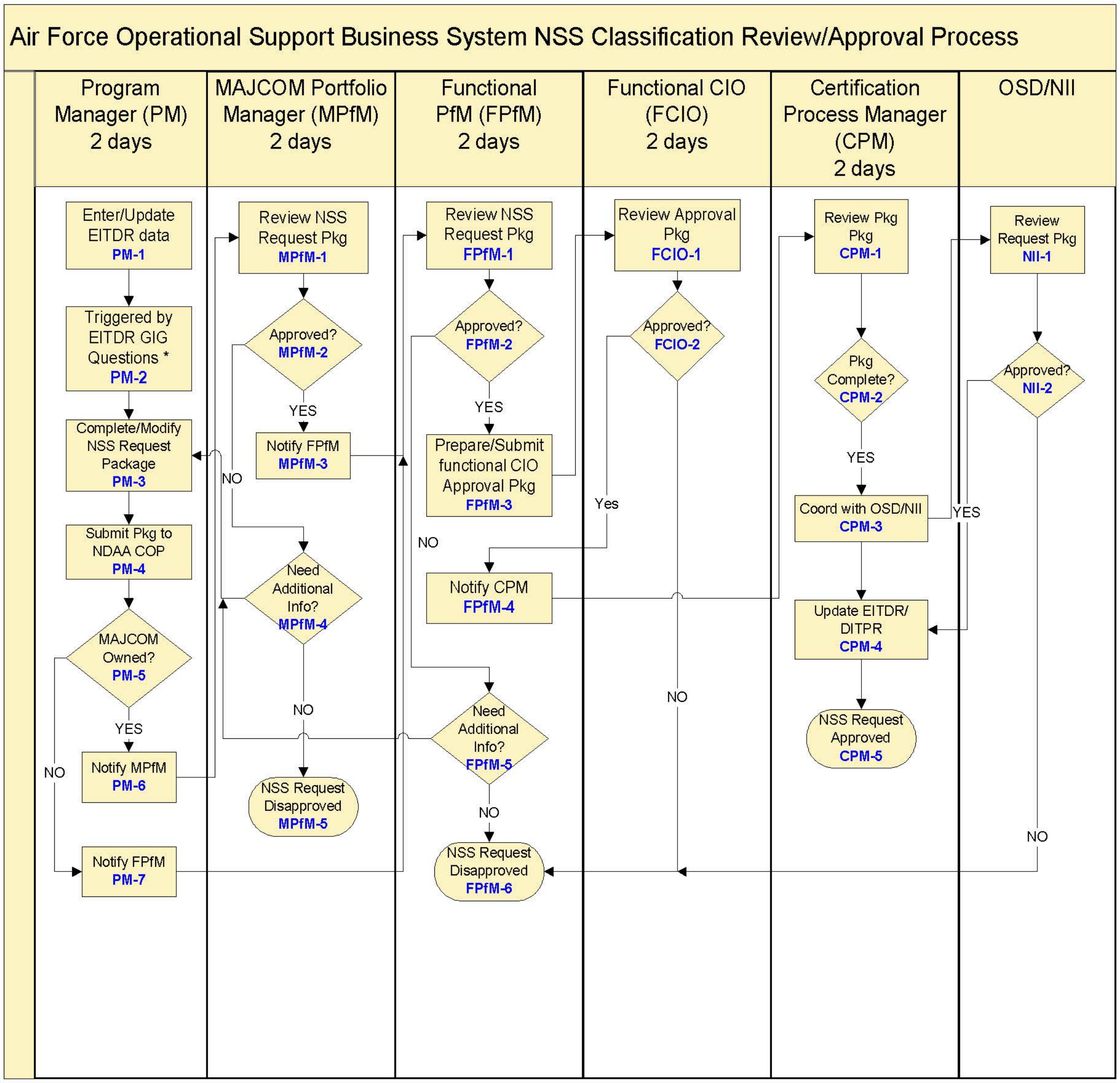
Air Force Operational Support Business System NSS Classification Review/Approval Process
Program Manager (PM) 2 days
MAJCOM Portfolio Manager (MPfM) 2 days
Functional PfM (FPfM) 2 days
Functional CIO (FCIO) 2 days
Certification Process Manager (CPM) 2 days
OSD/NII
Enter/Update EITDR data PM-1
Triggered by EITDR GIG Questions * PM-2
Complete/Modify NSS Request Package PM-3
Submit Pkg to NDAA COP PM-4
MAJCOM Owned? PM-5
YES
NO
Notify MPfM PM-6
Notify FPfM PM-7
Review NSS Request Pkg MPfM-1
Approved? MPfM-2
YES
NO
Notify FPfM MPfM-3
Need Additional Info? MPfM-4
NO
NSS Request Disapproved MPfM-5
Review NSS Request Pkg FPfM-1
Approved? FPfM-2
YES
NO
Prepare/Submit functional CIO Approval Pkg FPfM-3
Notify CPM FPfM-4
Need Additional Info? FPfM-5
NO
NSS Request Disapproved FPfM-6
Review Approval Pkg FCIO-1
Approved? FCIO-2
Yes
NO
Review Pkg Pkg CPM-1
Pkg Complete? CPM-2
YES
Coord with OSD/NII CPM-3
Update EITDR/ DITPR CPM-4
NSS Request Approved CPM-5
Review Request Pkg NII-1
Approved? NII-2
YES
NO

Exhibit 1. Air Force Operational Support Business System NSS Classification Review/Approval Process.

AUDIT SCOPE

Audit Coverage. We accomplished audit work at Air Force Secretariat SAF/CIO A6, Air Force Headquarters (AF/A3O), 6 Major Commands, 3 Field Operating Agencies and 10 installation organizations (Appendix III). We performed the review from January 2011 through June 2011 using documents dated from December 1995 through May 2011. We provided a draft report to management in August 2011.

Sampling Methodology. We used the following sampling concepts and Computer-Assisted Auditing Tools and Techniques (CAATTs) to complete this audit:

- **Sampling.**

  - Identification. As of 4 November 2010, the EITDR contained 422 IT systems and initiatives identified as NSS. Initially, we randomly selected 60 of 422 for review. However, our statistician modified our original sample to remove specific Pacific Air Forces (PACAF)[5] unique IT systems resulting in a modified universe of 367 with a sample size of 28 systems.

  - In addition, we judgmentally expanded our sample in three areas:

    - First, we judgmentally selected the AFWA based on auditor expertise and known potential issues. We reviewed 30 systems classified as NSS at AFWA.

    - Second, we expanded our sample to include SIPRNet circuit enclaves (infrastructure) included in EITDR based on an initial indication of a problem observed in our original random sample. As a result, we reviewed 243 SIPRNet circuit enclaves.

    - Third, we expanded our sample to include VTC, another infrastructure, listed in EITDR based on an observations made with our initial random sample. As a result, we reviewed 98 VTCs.

- **CAATTs.** We used advanced features of the Microsoft Excel® worksheet program to summarize and sort NSS identification and classification information from the EITDR.

[5] The sample modification was made to accommodate real world tsunami and earthquakes in the PACAF region.

Data Reliability. We extensively relied on computer-processed data contained in the EITDR. To establish data reliability, we compared output data to manual documents to validate data accuracy; and reviewed output products for obvious errors, reasonableness, and completeness. Based on these tests, we concluded that the data were reliable in meeting the audit objective.

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 audit results and conclusions based on the stated objectives. We believe the evidence obtained provides a reasonable basis for the audit results and conclusions cited in this report.

Internal Controls. We reviewed internal controls to determine whether the Air Force effectively classified national security systems. Specifically, we reviewed the effectiveness of the classification review and approval process and oversight used to classify national security systems.

PRIOR AUDIT COVERAGE

We did not identify any Air Force Audit Agency, DoD Inspector General, Government Accountability Office, or public accounting audit reports issued to management within the last 5 years that had related objectives.

Organization/Location	Installation-Level Reports Issued
Deputy Assistant Secretary (Financial Operations) (SAF/CIO A6)	NONE
Deputy Chief of Staff (Air, Space and Information Operations, Plans and Requirements, Directorate of Operations) (AF/A3O)	NONE
Air Force Materiel Command (AFMC)	
HQ AFMC Wright-Patterson AFB OH	NONE
Aeronautical Systems Center Wright-Patterson AFB OH	NONE
Arnold Engineering Development Center Arnold AFB TN	NONE
Ogden Air Logistics Center Hill AFB UT	NONE
Warner Robins Air Logistics Center Robins AFB GA	NONE
46th Test Wing Eglin AFB FL	NONE
95th Air Base Wing Edwards AFB CA	NONE
653d Electronic Systems Wing Hanscom AFB MA	NONE
Air Force Space Command (AFSPC)	
HQ AFSPC Peterson AFB CO	NONE

Organization/Location	**Installation-Level Reports Issued**
Air Force Space Command (AFSPC) (Cont'd)	
Air Force Network Integration Center Scott AFB IL	NONE
Space and Missile Systems Center Los Angeles AFB CA	NONE
50th Space Wing Schriever AFB CO	NONE
Air Force Special Operation Command	
1st Special Operations Wing Hurlburt Field FL	NONE
Air Mobility Command (AMC)	
HQ AMC Scott AFB IL	NONE
National Guard Bureau	
HQ ANG, National Guard Bureau Joint Base Andrews MD	NONE
Pacific Air Forces (PACAF)	
Joint Base Elmendorf Richardson Elmendorf AFB AK	NONE
Field Operating Agencies	
HQ Air Force Office of Special Investigation Andrews AFB MD	NONE
Air Force Intelligence, Surveillance, and Reconnaissance Agency Lackland AFB TX	NONE

Organization/Location	**Installation-Level Reports Issued**
Field Operating Agencies (Cont'd)	
Air Force Weather Agency Offutt AFB NE	F2011-0055-FBL000 10 June 2011

Points of Contact

Information Systems Development Division (AFAA/FSD)
Financial and Systems Audits Directorate
501 Ward Street
Maxwell AFB-Gunter Annex AL 36114-3236

[redacted], Program Manager
DSN [redacted]
Commercial [redacted]

[redacted], Audit Manager

We accomplished this audit under project number F2011-FB2000-0106.000.

Final Report Distribution

SAF/OS
SAF/US
SAF/FM
SAF/IG
SAF/LL
SAF/PA
SAF/A6 CIO
AF/CC
AF/CV
AF/CVA
AF/A4/7
AF/A6
AF/A8
AF/RE
NGB/CF

ACC
AETC
AFGSC
AFISR
AFMA
AFMC
AFOSI
AFRC
AFSOC
AFSPC
AMC
ANG
PACAF
USAFA
USAFE

AU Library
DoD Comptroller
OMB

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.

To request copies of this report or to suggest audit topics for future audits, contact the Operations Directorate at reports@pentagon.af.mil. Common Access Card users may download copies of audit reports from our Air Force Knowledge Now page at https://afkm.wpafb.af.mil/community/views/home.aspx?Filter=OO-AD-01-41.

Finally, you may mail requests to:

Air Force Audit Agency
Operations Directorate
1500 West Perimeter Road, Suite 4700
Joint Base Andrews MD 20762