FOLLOW-UP AUDIT, AIR FORCE EQUIPMENT MANAGEMENT SYSTEM CONTROLS
INTRODUCTION
The Air Force Equipment Management System (AFEMS) is an asset management system. It converts asset inventory activity to general ledger detail transactions, posts the transactions to general ledger accounts and provides the net change of general ledger balances to the Defense Finance Accounting Systems for Air Force financial statement reporting. The AFEMS reported asset values of over $38 billion in November 2008.

Portions of the AFEMS will migrate to Expeditionary Combat Support System (ECSS) in Fiscal Year 2012. However, AFEMS includes a classified portion that will not migrate to ECSS, and will continue as the Air Force system for managing classified assets.

OBJECTIVES
The Assistant Secretary of the Air Force, Financial Management and Comptroller requested this follow-up audit to determine whether the AFEMS program office took corrective actions in response to Recommendations A.1, A.2, B.1, B.2, and B.3 in Report of Audit, Air Force Equipment Management System Controls, F2006-0011-FB2000, 25 September 2006, and whether the actions taken were effective. Specifically, we determined whether AFEMS program office personnel:

- Performed risk analysis, effectively implemented system controls and obtained approval to operate.
- Complied with applicable federal accounting standards to identify design, test, and implement applicable federal accounting conformance requirements.

CONCLUSIONS
The AFEMS program office personnel took corrective actions for three of the five recommendations. Specifically, program office personnel performed risk analysis, obtained approval to operate, and modified the AFEMS
support contract statement of work to include DFAS 7900.4-G transaction testing standards. However, they did not:

- Comply with applicable federal accounting standards to design, test, and implement applicable federal accounting conformance requirements. Complete design, testing, and implementation of applicable accounting conformance requirements provide reasonable assurance the system processes transactions according to established accounting standards (repeat condition). (Tab A, page 1)

- Effectively implement three of seven system control areas (access controls, security program, and service continuity). Thoroughly implementing all applicable system controls enhances management oversight of $38 billion of Air Force assets to include nuclear weapon support equipment. (Tab B, page 4)

**RECOMMENDATIONS**

We made three recommendations to strengthen and enhance accounting conformance requirements and system controls. (Reference the individual Tabs for specific recommendations.)

**MANAGEMENT’S RESPONSE**

Management concurred with the intent of the audit results in Tab A and concurred with the audit results in Tab B. Management concurred with the intent of recommendation A.1 and provided alternative corrective actions, and concurred with recommendations B.1 and B.2 Management actions planned should correct the problems identified. Therefore, this report contains no issues requiring elevation for resolution.

RONALD J. PRENTKIEWICZ  
Associate Director  
( Information Systems Development Division )

JUDITH L. SIMON  
Assistant Auditor General  
( Financial and Systems Audits )
<table>
<thead>
<tr>
<th>Table of Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>i</td>
</tr>
<tr>
<td>TAB</td>
<td></td>
</tr>
<tr>
<td>A Accounting Conformance</td>
<td>1</td>
</tr>
<tr>
<td>B System Controls</td>
<td>3</td>
</tr>
<tr>
<td>APPENDIX</td>
<td></td>
</tr>
<tr>
<td>I Background Information</td>
<td>9</td>
</tr>
<tr>
<td>II Audit Scope and Prior Audit Coverage</td>
<td>13</td>
</tr>
<tr>
<td>III Locations Audited/Reports Issued</td>
<td>15</td>
</tr>
<tr>
<td>IV Points of Contact</td>
<td>17</td>
</tr>
<tr>
<td>V Final Report Distribution</td>
<td>19</td>
</tr>
</tbody>
</table>
BACKGROUND


DFAS summarizes applicable accounting requirements in DFAS 7900.4-G, Version 6.0. The Guide applies to accounting and finance systems as well as “feeder” systems and military services and DoD component agencies systems supporting other functional areas. The program office must review the guide, select requirements applicable to the system, and implement the selected requirements when planning, designing, enhancing, or modifying financial management systems. The AFEMS program office personnel identified two chapters applicable to AFEMS.

- Chapter 3, Property, Plant, and Equipment Controls, discusses system requirements to account for assets, assess the condition of assets, as well as provide an audit trail. In addition, this chapter discusses the flow of accounting information for depreciation.

- Chapter 14, Audit Trails and System Controls, addresses system requirements to provide audit trails to trace transactions from their initial source through all stages of related system processing, and identify document input, change, approval, and user deletions. In addition, the system administrator must be able to define assigned user identification, functional role, and owner organization functional access rights (to modules, transactions, and approval authorities) and data access rights (create, read, update, and delete records).

AUDIT RESULTS 1 – ACCOUNTING CONFORMANCE

Condition. The AFEMS program office personnel did not comply with applicable federal accounting standards to test and implement applicable federal accounting conformance requirements. Although program office personnel identified 123 accounting conformance requirements, available documentation supported the successful testing and implementation of only 15 requirements. To illustrate, program office personnel identified each of the following requirements as applicable to AFEMS; however, they did not have test scripts, test reports or any other documentation to support requirements testing and implementation. This is a repeat condition from Air Force Audit Agency (AFAA) Report of Audit F2006-0011-FB2000, 25 September 2006, Tab B, page 7.
Tab A
Accounting Conformance

- **Acquisition Cost.** The property system should record the acquisition of a general Property, Plant, and Equipment (PP&E) asset with a dollar value supported by appropriate documentation. Documentation (original documents and/or hard and electronic copies of original documentation) shall be maintained in a readily available location during the applicable retention period.

- **Asset Life.** The property system must be able to record the estimated useful life of an asset for depreciation purposes based on the DoD standard recovery period.

- **Depreciation Accumulation.** The property system must accumulate depreciation expense in a contra asset account: accumulated depreciation. It must also accumulate amortization expense in a contra asset account: accumulated amortization.

**Cause.** This condition occurred because the system owner (Air Force Directorate of Logistics, Directorate of Transformation, AF/A4I) did not fund the requirements testing as recommended in the previous report of audit. (Report of Audit F2006-0011-FB2000, 25 September 2006, Tab A, Recommendation A.1 and Tab B, Recommendation B.2.)

**Impact.** Complete design, testing, and implementation of applicable accounting conformance requirements provide reasonable assurance the system processes transactions according to established accounting standards.

**Recommendation A.1.** The AF/A4I should provide funding and require the AFEMS program office to design, test, implement and document each applicable accounting conformance requirement.

**Management Comments.** The Air Force Directorate of Logistics, Directorate of Transformation (AF/A4I) concurred with intent and stated: “AFEMS was not funded to support testing to confirm CFO compliance because the Expeditionary Combat Support System, which will replace AFEMS capability, was scheduled for fielding in 2010. As of 1 April 2008, AFEMS was placed in a soft freeze for software as it will be one of the first increments to be transitioned to ECSS, consequently, only AF/A4RB approved software changes can be implemented. If for some reason ECSS becomes “at risk” for implementation and AFEMS is retained as the system of record, CFO compliance issues will be addressed. Closed.”

**Evaluation of Management Comments.** Management comments addressed the issues raised in the audit results, and offered alternative corrective actions for Recommendation A.1 that when implemented, should correct the problem.
BACKGROUND

Systems controls safeguard information systems against loss and unauthorized use or misappropriation of resources and information. The Government Accountability Office (GAO) "Federal Information System Controls Audit Manual" (FISCAM) emphasizes 10 critical system control areas that, if effectively implemented, help ensure successful system development and operational performance. Further, the FISCAM provides management and systems’ auditors guidance for evaluating the general and application controls that directly impact the integrity, confidentiality, and availability of data maintained in computer-based information systems. (See Appendix I for a complete list and detailed explanation of system controls.)

The DoD Instruction\(^1\) (DoDI) 8500.2 requires the program office establish and implement a comprehensive account management process to ensure only authorized users can gain access to workstations, applications, and networks and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated. The program office should establish procedures to disable all accounts with inactivity exceeding 45 days, and delete all disabled accounts 90 days from the date they were disabled.\(^2\) All AFEMS contract personnel assigned to positions designated as Information Technology category one (IT-I) require a Single Scope Background Investigation while performing their duties.\(^3\) Data Base Administrators, Systems Administrators and Computer Operators are positions designated IT-I.

The Program Manager develops a Plan of Action and Milestones (POA&M) to document resources required to accomplish corrective actions and meet projected milestones and completion dates as part of the certification and accreditation process. Program managers and information assurance personnel use the POA&M to identify, assess, prioritize, and monitor efforts to correct program and system security vulnerabilities. The Air Force Chief Information Officer (CIO), Secretary of the Air Force for Warfighting Integration and Chief Information Officer, Enterprise Networks Division (SAF/XCPP), monitors and tracks the execution of system-level IT Security POA&Ms until identified security weaknesses have been closed and the Certification and Accreditation (C&A) documentation

\(^1\) The DoDI 8500.2, Information Assurance (IA) Implementation, Attachment 5 to Enclosure 4, Confidentiality Controls for DoD Information Systems Processing Sensitive Information, control number IAAC-1, 6 February 2003.


\(^3\) DoDI 8500.2, Table E3.T1., Investigative Levels for User with IA Management Access to DoD Unclassified Information Systems.
appropriately adjusted. The Program Manager implements corrective actions identified in the POA&M and reports the status of corrective actions to the Air Force CIO. The AFEMS POA&M reflects vulnerabilities for both the classified and unclassified side.

Losing the capability to process, retrieve, and protect information maintained electronically can significantly impact an agency’s ability to accomplish its mission. For this reason, an agency must have contingency plans in place to protect information resources, minimize the risk of unplanned interruptions, and provide data back-up in order to recover critical operations should interruptions occur. These plans should consider the activities performed at data processing centers as well as user performance of specific applications. Management should periodically test recovery plans using disaster simulation exercises.

**AUDIT RESULTS 2 – SYSTEM CONTROLS**

**Condition.** The AFEMS program office personnel did not effectively implement three of seven system control (access controls, security program planning and management controls, and service continuity controls).

- **Access Controls.** The AFEMS program office personnel did not effectively monitor system access and delete inactive user accounts. For example, 549 personnel had not used their accounts in over a year, and 4,698 personnel had approved accounts created from July 2000 through October 2008, but had never accessed the system.

- **Security Program Planning and Management Controls.** The AFEMS program office personnel did not effectively manage Security Program Planning and Management Controls. Specifically:
  - **Security Investigations.** Program office personnel granted contractors access to the system and Secret Internet Protocol Router Network (SIPRNET) without first completing required security investigations. Although the Air Force and contractor signed the AFEMS contract in March 2008, in December 2008 14 of 27 contractor personnel did not have the required current investigations initiated in the Joint Personnel Adjudication System. In addition, the pro-

---

4 DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, paragraph 6.3.2.4, 28 November 2007.

5 The Joint Personnel Adjudication System (JPAS) is a DoD web-based system that connects security personnel around the world with a database managed by DoD Agency Central Adjudication Facilities. JPAS provides “real-time” information regarding clearance, access and investigative status to authorized DoD security personnel.
program office gave 11 of these 14 individuals access to the SIPRNET prior to completion of a Single Scope Background Investigation required by DoD directive guidance and the contract.6

- **Plan of Action and Milestones (POA&M).** The AFEMS program office personnel did not prepare POA&Ms to report all system vulnerabilities to the Air Force CIO and certifying authorities. To illustrate, program office personnel only reported two system vulnerabilities to SAF/XCPP. However, available documentation demonstrated that program office personnel were aware of 28 additional vulnerabilities. These vulnerabilities were identical for both the classified and unclassified side.

- **Service Continuity Controls.** Service continuity controls required improvement. Specifically, system program personnel did not:

  - **Alternate Site-Backup Data.** Identify an alternate site, create a memorandum of understanding with this site and execute backup procedures to store data at the alternate site.

  - **Contingency Plan Testing.** Thoroughly test the contingency plan. For example, testing was limited to tabletop scenarios and never demonstrated actual ability to resume operations at an alternate facility.

**Cause.** These conditions occurred because the program manager did not establish procedures to ensure the contractor:

- Deleted inactive user accounts.

- Obtained the required SSBI background investigations and clearances.

- Complied with POA&M reporting requirements.

In addition, the system owner (AF/A4I) did not provide funding to identify an alternate backup site, establish a memorandum of understanding with the alternate site for contingency operations, and execute backup procedures to ensure system resource availability at the alternate site in the event of the need to execute the contingency plan.

**Impact.** Thoroughly implementing all applicable system controls enhances the oversight of $38 billion of Air Force assets to include nuclear weapon support equipment. Specifically:

---

6 Each of the 11 contractors did have a Secret clearance granted on a different type of investigation.
Maintaining the highest level of contractor security provides assurance that contractors are free of criminal activity and potential terrorist connections.

Accurately identifying the classified and unclassified weaknesses, associated resources, and timeframes required to complete corrective actions in PO&AMs facilitate system security weakness mitigation. Identifying and mitigating security vulnerabilities protect the confidentiality, integrity, and availability of Air Force information and information systems.

Annually exercising contingency plans helps identify, mitigate, and resolve shortfalls in procedures or resources. This includes alternate facilities, staffing, equipment, or training needed to sustain or timely restore network operations during or following a contingency.

Recommendation B.1. The Director, 754th Electronic Systems Group (HQ 754 ELSG) should require the program office manager to establish procedures to ensure the contractor:

a. Deletes inactive user accounts.

b. Obtains the required Single Scope Background Investigations (SSBI) background investigations and clearances.

c. Complies with POA&M reporting requirements and report all vulnerabilities.

d. Develops an alternate site plan.

e. Establishes back up procedures in the contingency plan.

f. Thoroughly tests the contingency plan.

Management Comments. The Director of Transformation, DCS/Logistics, Installations, and Mission Support concurred and stated:

a. “A4I issued account management instructions to all logistics systems program offices and ALCs on 11 May 2009 with a 15 June 2009 suspense to delete all inactive system accounts. A4IS is in the process of tracking responses, identifying problems and managing solutions. We will follow-up in cases where the system is incapable of automating the account management function and periodically assess compliance. This task requires PMO review of user accounts every 30 days. We anticipate compliance within the next 6-months. Estimated Completion Date: 16 January 2010.”
b. “DoDI 8500.2 and AFI 31-501 are not consistent with DoD 5200.2-R concerning investigative requirements for IT I level specialist. DoD 5200.2-R, paragraph C2.3.6 require personnel holding a critical sensitive position (IT I level specialist) have a Background Investigation (BI). DoDI 8500.2 mentions the DoD 5200.2-R requirement, but Table E3.T1 requires IT I level contractors to have a Single Scope BI (SSBI). A4I will engage SAF/XC to resolve this discrepancy.

AFEMS contractors had secret clearances required to access the SIPRNet and AFEMS classified data, but lacked the necessary background investigation required of IT I level personnel. AFEMS contractors are required to pass a BI by DoD 5200.2-R or a SSBI by DoDI 8500.2 standards. The AFEMS PMO will ensure all contractors with IT I level responsibilities are processed for the SSBI until DoD resolves inconsistence between DoD 5200.2-R and DoDI 8500.2.

The PMO will submit the last two SSBI contractor packages by 14 August 2009 and is optimistic OPM will complete the four ongoing investigations by 1 October 2009. All AFEMS contractors with IT I level responsibilities will have adjudicated SSBI by 1 January 2010. Estimated Completion Date: 16 January 2010.

c. “The AFEMS PMO is in the process of re-accrediting the system through the IT LEAN process. The IT LEAN process now self-generates the necessary POAM which is validated by AFCA and reported to SAF/XC. Upon completion of the IT LEAN process this fall, AFEMS will be compliant with the requirement to establish a POAM, reporting vulnerabilities to SAF/XC. Estimated Completion Date: 16 January 2010.

d. “The AFEMS PMO will develop a plan to reestablish AFEMS at an alternate computing site to support the process within 72 hours of a catastrophic event at the primary computing enclave. Estimated Completion Date: 16 January 2010.

e. “AFEMS is a Mission Assurance Category (MAC) II system and must backup system data daily, storing this database off site. The AFEMS Contingency Plan contains necessary tasks to ensure AFEMS data is available at the alternate site. Estimated Completion Date: 16 January 2010.

f. “AFEMS is a MAC II system required to identify an alternate computing site for contingency operations. The AFEMS PMO will be directed to designate an alternate computing site so the Contingency Plan walk-through can undergo meaningful table top testing. Estimated Completion Date: 16 January 2010.”
**Recommendation B.2.** AF/A4I should provide funding and task the program manager to:

a. Identify an alternate site.

b. Establish a memorandum of understanding with the alternate site for contingency operations.

c. Execute backup procedures to ensure availability of system resources at the alternate site.

**Management Comments.** The Director of Transformation, DCS/Logistics, Installations, and Mission Support concurred and stated:

a. “AFEMS is a MAC II system, which requires PMO to identify an alternate site for system operation. The PMO will be instructed to identify a computing enclave capable of hosting AFEMS and the AFEMS database and capable of reestablishing necessary interfaces with all boundary protections currently provided at the primary site. Movement and system reconstitution must be accomplished within 72 hours in order to support the AFEMS Business Impact Analysis. Estimated Completion Date: 16 January 2010.

b. “AFEMS is a MAC II system, which requires PMO to identify an alternate site for system operation. The PMO will execute the necessary Service Level Agreement, integrating these changes in the current IT Contingency Plan. We expect these tasks to be accomplished within the next six months. Estimated Completion Date: 16 January 2010.

c. “AFEMS is a MAC II system, which requires PMO to identify an alternate site for system operation. Current data backup procedures comply with DoD and Air Force guidance for MAC II system. Backup applications and database files are secured off the primary computing site as required backups are accomplished daily and these files are easily available for transfer to any alternate site. Estimated Completion Date: 16 January 2010.”

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

The Financial Systems Integration Office (formally known as the Joint Financial Management Improvement Program) develops, tests and certifies federal financial management system requirements. The DFAS Guide .4G provides a comprehensive compilation of financial management systems requirements mandated by the Federal Financial Management Improvement Act of 1996. Requirements contained within this document are applicable to accounting and finance systems operated and maintained by DFAS as well as “feeder” systems owned by the military services and DoD component agencies. The Guide includes 16 chapters of accounting processes related to virtually every type of accounting system.

SYSTEM CONTROLS

The Federal Information System Control Audit Manual (FISCAM) provides a GAO-developed methodology for assessing computer-processed data from financial management systems, as called for in Government Auditing Standards. The general methodology used in the FISCAM involves evaluating general and application system controls. General controls are the policies and procedures that apply to all or a large segment of an entity’s information systems and help ensure their proper operation. These controls include entity-wide security program planning and management controls, access controls, confidentiality controls, application software development and change controls, segregation of duties controls, service continuity controls, completeness controls, and accuracy controls. Application controls relate to individual computerized applications and include authorization controls, completeness controls, accuracy controls, and confidentiality controls. The following paragraphs describe critical elements within these ten system control categories:

- **Entity-wide Security Program Planning and Management Controls.** Entity-wide security program planning and management control provides a framework and continuing cycle of activity for assessing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity’s computer-related controls. The SSAA documents the system security program. PMO personnel must obtain an accredited SSAA prior to initial operation and at least every 3 years thereafter.

- **Access Controls.** Access controls limit or detect access to computer resources (data, programs, equipment, and facilities) thereby protecting these resources against unauthorized modification, loss, and disclosure. Examples of access controls include documentation of user access and associated permissions, enforcement of password format requirements, periodic reviews of user access, and access restrictions over system security software.
• **Application Software Development and Change Controls.** Application software development and change controls prevent implementation of unauthorized programs or modifications to an existing program. These controls include the documentation process that records information produced by a life cycle methodology or activity. The documentation should be current and of sufficient scope and depth to provide managers, users, system operators, and software maintenance personnel with an understanding of the system.

• **System Software Controls.** System software controls limit and monitor access to the programs and sensitive files that control the computer hardware and secure applications supported by the system. Software patches and updates help ensure the continued protection of these programs and files. The system software monitors access through logging of user access and user identification and permission changes.

• **Segregation of Duties Controls.** Segregation of duties are policies, procedures, and an organizational structure established so one individual cannot control key aspects of computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records.

• **Service Continuity Controls.** Service continuity controls ensure when unexpected events occur, the system continues or promptly resumes critical operations, and protects critical and sensitive data. PMO personnel should clearly document a contingency plan, communicate it to the staff, test the plan, and update it to reflect current operations.

• **Authorization Controls.** Authorization Controls ensure only valid transactions, those representing events that actually occurred in accordance with management’s general and specific permission, are authorized for processing. For financial reporting purposes, authorization control objectives relate directly to the existence or occurrence assertion.

• **Completeness Controls.** These control objectives complement the authorization control objectives in they address the risk that the system does not process all valid and authorized transactions. For financial reporting purposes, these controls related directly to the completeness assertion.

• **Accuracy Controls.** The system must record financial data at correct amounts, and non-financial data at correct values. Accuracy control objectives help ensure proper recording. For financial reporting purposes, these control objectives relate directly to the valuation or allocation assertion.
- **Confidentiality Controls.** Many entities, both governmental and nongovernmental, face increased pressure to maintain the confidentiality of information it collects about its customers, business partners, and other constituents. Control objectives that address confidentiality do not have a direct effect on financial reporting, but they can be an important element of helping the entity achieve operational objectives and comply with laws and regulations.
Audit Scope and Prior Audit Coverage

AUDIT SCOPE

Audit Coverage. We accomplished audit work at the 754 ELSG system program office located at Headquarters Air Force Materiel Command (Appendix III). We conducted this audit from June 2008 through March 2009 using documentation supporting AFEMS accounting functions from July 2005 through March 2008. We provided a draft report to management in May 2009. Specifically:

- Contract Modification. To determine whether program office personnel modified the AFEMS support contract statement of work to include DFAS 7900.4-G transaction testing we obtained the current contract, reviewed the statement of work, and verified the statement of work included a contract line item number for DFAS 7900.4-G transaction testing. Next, we obtained the approval to operate and verified the signature and date.

- Accounting Conformance. To determine whether program office personnel established and implemented procedures to verify and document the design, test and implementation of applicable accounting conformance requirements we requested the test scripts to support 123 identified accounting conformance requirements. Management provided test scripts located in the System Security Authorization Agreement (SSAA) supporting 17 security related tests. We only reviewed 15 (of the 17) test results in the SSAA that had passed an internal DFAS 7900.4-G review.

- System Controls. To determine whether program office personnel performed risk analysis and corrected system control deficiencies, we judgmentally selected seven controls areas (security program, access, change, segregation of duties, service continuity, accuracy and confidentiality). We then tested 20 critical elements of these control areas for deficiencies. To accomplish this we verified user access listings and whether personnel still required system access. We obtained the SSAA and POA&M and verified SSAA analysis identified each risk and the POA&M reported the risk and the estimated date to correct the deficiency. We verified the program office was reporting the POA&M data to higher headquarters. Finally, we reviewed contingency plan documentation for an alternate site, data backup procedures, and contingency plan testing.

Sampling Methodology. We did not use sampling or Computer Assisted Auditing Tools and Techniques during this review.

---

7 We did not select authorization, completeness, and system software controls to avoid duplication with a planned audit of internal use software that would cover these application controls.
Audit Scope and
Prior Audit Coverage

Data Reliability. We extensively relied on computer-processed data contained in AFEMS. To assess data reliability, we compared output data to manual documents to validate data accuracy, and reviewed user privilege output products for obvious errors, reasonableness, and completeness. Based on these tests, we concluded the data were sufficiently reliable to support audit conclusions.

Auditing Standards. We conducted this audit in accordance with generally accepted government auditing standards and, accordingly, included AFEMS system control tests. Specifically, we evaluated internal controls related to security program efficiency, access controls, application software development and change controls, confidentiality controls, segregation of duties, service continuity controls, completeness controls, and accuracy controls.

PRIOR AUDIT COVERAGE

We did not identify any DoD Inspector General or Government Accountability Office reports issued within the last 5 years that addressed the same or similar objectives as this audit. However, we did identify the following AFAA report with similar objectives.

- AFAA Report of Audit F2006-0011-FB2000, Air Force Equipment Management System Controls, 25 September 2006, determined whether personnel maintained (a) system controls including risk assessments and general and application controls, and (b) accounting conformance requirements to comply with applicable federal accounting standards. The report made three recommendations to strengthen system controls and three recommendations to conduct a DFAS Blue-book evaluation to identify, design, and test applicable federal accounting conformance requirements. Although management officials conducted the recommended Bluebook evaluation, modified the AFEMS support contract statement of work to include DFAS 7900.4-G transaction testing standards, performed risk analysis, and obtained approval to operate, they did not effectively implement all recommendations. Repeat conditions are discussed on page one of this report.
<table>
<thead>
<tr>
<th>Organization/Location</th>
<th>Installation-Level Reports Issued</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Air Force Materiel Command</strong></td>
<td></td>
</tr>
<tr>
<td>754 ELSG</td>
<td></td>
</tr>
<tr>
<td>Wright-Patterson AFB OH</td>
<td></td>
</tr>
</tbody>
</table>

*We did not issue installation-level reports during this review.*
Points of Contact

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

Ronald J. Prentkiewicz, Associate Director
DSN 596-5107
Commercial (334) 416-5107

Raymond Harris, Program Manager

John E. Andrews Jr., Audit Manager

We accomplished this audit under project number F2008-FB2000-0062.000
This Page Intentionally Left Blank
Final Report Distribution

<table>
<thead>
<tr>
<th>SAF/OS</th>
<th>ACC</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAF/US</td>
<td>AETC</td>
</tr>
<tr>
<td>SAF/FM</td>
<td>AFDW</td>
</tr>
<tr>
<td>SAF/IG</td>
<td>AFCESA</td>
</tr>
<tr>
<td>SAF/LL</td>
<td>AFMA</td>
</tr>
<tr>
<td>SAF/PA</td>
<td>AFMC</td>
</tr>
<tr>
<td>SAF/XC, AF/A6</td>
<td>AFOSI</td>
</tr>
<tr>
<td>AF/CC</td>
<td>AFRC</td>
</tr>
<tr>
<td>AF/CV</td>
<td>AFSOC</td>
</tr>
<tr>
<td>AF/CVA</td>
<td>AFSPC</td>
</tr>
<tr>
<td>AF/A4</td>
<td>AFISR</td>
</tr>
<tr>
<td>AF/A8</td>
<td>AMC</td>
</tr>
<tr>
<td>AF/RE</td>
<td>ANG</td>
</tr>
<tr>
<td>NGB/CF</td>
<td>PACAF</td>
</tr>
<tr>
<td>AU Library</td>
<td>USAFA</td>
</tr>
<tr>
<td>DoD Comptroller</td>
<td>USAFE</td>
</tr>
<tr>
<td>OMB</td>
<td>Units/Orgs Audited</td>
</tr>
</tbody>
</table>

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 (703) 696-7913 (DSN 426-7913) or E-mail to reports@pentagon.af.mil. Certain government users may download copies of audit reports from our home page at www.afaa.hq.af.mil/. Finally, you may mail requests to:

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