~~FOR OFFICIAL USE ONLY~~

September 21, 2004

Information System Security

The Followup on the Government Accountability Office and U.S. Army Audit Agency Recommendations for the U.S. Army Corps of Engineers

(D-2004-115)

SPECIAL WARNING

~~This report contains information exempt from mandatory disclosure under the Freedom of Information Act, Exemption 2.~~

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

~~FOR OFFICIAL USE ONLY~~

Additional Copies

To obtain additional copies of this report, visit the Web site of the Inspector General of the Department of Defense at http://www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit, Audit Followup and Technical Support at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact Audit Followup and Technical Support at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General of the Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

September 21, 2004

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE
(COMPTROLLER)/CHIEF FINANCIAL OFFICER
COMMANDING GENERAL, ARMY CORPS OF
ENGINEERS

SUBJECT: Report on the Followup on the Government Accountability Office and U.S. Army Audit Agency Recommendations for the U.S. Army Corps of Engineers (Report No. D-2004-115)

We are providing this report for review and comment. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Commanding General, Army Corps of Engineers (U.S. Army Corps of Engineers) comments were partially responsive. We request additional comments on Recommendations 1.j., 1.l., 2.b., 2.i., 2.j., and the dates that the actions will be completed. We request that the Commanding General, Army Corps of Engineers provide comments on this final report by October 6, 2004.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to Auddfs@dodig.osd.mil. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Questions should be directed to (b) (6) [redacted] at (703) 604-(b) (6) [redacted] (DSN 664-(b) (6) [redacted] or (b) (6) [redacted] at (703) 604-(b) (6) [redacted] (DSN 664-(b) (6) [redacted] See Appendix F for the report distribution. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Paul J. Granetto, CPA
Assistant Inspector General
Defense Financial Auditing
Service

Office of the Inspector General of the Department of Defense

Report No. D-2004-115 **September 21, 2004**
(Project No. D2003FG-0139.000)

The Followup on the Government Accountability Office and U.S. Army Audit Agency Recommendations for the U.S. Army Corps of Engineers

Executive Summary

Who Should Read This Report and Why? DoD personnel who manage and use the U.S. Army Corps of Engineers (USACE) financial management system will find items of interest in this report, as will persons who supervise any part of the DoD information security program. The report follows up on the USACE responses to Government Accountability Office (GAO) and U.S. Army Audit Agency (AAA) audit recommendations, and discusses the need to further improve information assurance within USACE.

Background. The Under Secretary of Defense (Comptroller)/Chief Financial Officer requested that we follow up on the USACE progress in complying with the 62 recommendations made in GAO Report No. GAO-02-206, issued in March 2002, and in AAA Report No. A-2002-0610-FFC, issued in September 2002. GAO and AAA directed the recommendations to USACE Headquarters, USACE Financial Management System Systems Development and Maintenance Directorate, USACE Finance Center, and USACE data processing centers and districts. We will issue a separate report discussing the status of 14 recommendations directed to the districts.

Results. USACE had not fully implemented the 62 recommendations. Specifically, 14 recommendations were not implemented at all, and 23 other recommendations were only partially implemented. A USACE management-driven remediation plan with an effective information assurance program would have helped to ensure that all the recommendations were addressed. Instead, USACE information continues to be vulnerable to unauthorized access and damage. The Office of the Inspector General of the Department of Defense along with GAO and AAA, based their audit work on Army Regulation 380-19; however, the regulation was replaced by Army Regulation 25-2 on November 14, 2003. USACE managers must establish guiding principles for information assurance in full compliance with Federal laws and DoD and Army Regulations.

Management Comments and Audit Response. The USACE Command response for the Director of Corporate Information, Corps of Engineers Enterprise Infrastructure Services Program Management Office, Corps of Engineers Financial Management System Program Management Office, and Finance Center concurred with 43 of the 44 recommendations.

The USACE Command response for the Director of Corporate Information nonconcurred with 1 of the13 recommendations to the director. Specifically, the USACE Command did not agree to implement a secure and controllable manner to provide information to the customers that eliminates the need for the anonymous File Transfer Protocol. However, USACE proposed acceptable alternate solutions that satisfied the intent of the GAO recommendation.

The USACE Command response for the Corps of Engineers Enterprise Infrastructure Services Program Management Office concurred with the 16 recommendations to the program management office. In addition, the USACE Command response for the Corps of Engineers Financial Management System Program Management Office concurred with the two recommendations to the program management office. Finally, the USACE Command response for the Director of the Army Corps of Engineers Finance Center concurred with the 13 recommendations to the Finance Center.

Although USACE concurred with the recommendations, we do not fully agree with proposed actions or additional facts provided by USACE on five recommendations; and therefore, we request additional comments on the recommendations. Specifically, we do not agree that:

- the completion of Designated Approving Authority (DAA) training was tracked for DAAs and other personnel who require the training;

- one integrated continuity of operations plan for all USACE sites and major automated information systems was completed;

- physical security reviews of the Western Processing Center (WPC) were coordinated with the Portland District Security Office;

- risks associated with null connections were documented in the Corps of Engineers Enterprise Infrastructure Services (CEEIS) risk assessment, or that a plan was established to mitigate risks associated with null connections; and

- the change approval process provided a clear understanding of approving and disapproving authority.

We request that the Commanding General, Army Corps of Engineers provide comments on the final report by October 6, 2004. See the Finding section of the report for a discussion of management comments and the Management Comments section of the report for the complete text of the comments.

Table of Contents

Background

Followup Request. The audit was requested by the Under Secretary of Defense (Comptroller)/Chief Financial Officer to follow up on the 62 recommendations contained in the Government Accountability Office (GAO) Report (GAO-02-206), March 2002, and the U.S. Army Audit Agency (AAA) Report (A-2002-0610-FFC), September 2002. The recommendations were directed to the U.S. Army Corps of Engineers (USACE) Headquarters, Corps of Engineers Financial Management System (CEFMS) Systems Development and Maintenance Directorate, U.S. Army Corps of Engineers Finance Center (UFC), two data processing centers, and districts. A separate report will be issued discussing the recommendations that were validated at the USACE Headquarters, districts, and Transatlantic Center. The separate report will address the following areas:[1] Logical Access Controls, Segregation of Duties, Network Security, Application Controls, Entity-Wide Security, and Continuity of Operations.

Audit Approach. This report groups the recommendations into one of the following five categories: Implemented, Not Implemented, Partially Implemented, Could Not Implement, and USACE sites.[2]

We obtained assistance from the U.S. Army 1st Information Operations Command Vulnerability Assessment Division (external technical reviewers). The external technical reviewers assisted the audit team in the following areas: Logical Access Controls, System Software, Application Software Development and Change Control, and Network Security. We also obtained assistance from the Office of the Inspector General of the Department of Defense (IG DoD) Technical Assessment Division in the following areas: Logical Access Controls, System Software, Segregation of Duties, and Network Security. We determined the scope of the reviewers audit work, monitored their progress, and reviewed the related work papers.

A summary of the information security policy, acronyms, and GAO and AAA recommendations can be found in Appendices B, C, and D, respectively. GAO and AAA had based their audit work on Army Regulation (AR) 380-19, “Information Systems Security,” February 27, 1998, and our work was based on AR 380-19 as well. However, the Department of Army issued AR 25-2, “Information Assurance,” November 14, 2003, to replace AR 380-19. AR 25-2 provided more stringent requirements. For example, AR 25-2 requires passwords to be a minimum of 10 characters; however, AR 380-19 required them to be a minimum of eight characters. USACE must adapt and comply with the new Army Regulation and implement our recommendations in accordance with AR 25-2.

[1] Ten of the recommendations will be partially addressed in this report and the remaining parts of the recommendation will be addressed in our report on the USACE Headquarters, districts, and Transatlantic Center.

[2] USACE sites include the USACE Headquarters, districts, and Transatlantic Center.

Government Accountability Office. The GAO evaluated the design and tested the effectiveness of selected USACE general and application controls over CEFMS for FY 2001. Also, GAO assessed the corrective actions taken by USACE to address weaknesses that GAO identified during the FY 1999 review. Appendix I of the March 2002 GAO Report contained 53 recommendations-48 general control recommendations and 5 application control recommendations.[3]

U.S. Army Audit Agency. The AAA report evaluated the effectiveness of entity-wide security management and service continuity controls over CEFMS and evaluated the USACE implementation of recommendations made during the FY 1999 AAA review. The AAA report contained nine recommendations regarding entity-wide security and continuity of operation controls.

U.S. Army Corps of Engineers Financial Statements. USACE management asserted that the USACE FY 2003 financial statements were presented fairly in accordance with generally accepted accounting principles and were ready for audit. The General Accounting Office and the President's Council on Integrity and Efficiency Financial Audit Manual, July 2001, requires that auditors obtain an understanding of internal control sufficient to plan an audit of the entities' financial statements. Information systems general and application controls are critical to managing computer security and ensuring the reliability, confidentiality, and availability of sensitive financial data. The Federal Financial Management Improvement Act of 1996 was intended to advance Federal financial management by ensuring that Federal financial management systems provide reliable, consistent disclosure of financial data that is uniform across the Federal Government from year to year.

U.S. Army Corps of Engineers Financial Management System. CEFMS is the standard USACE field-level automated accounting and financial reporting system used for supporting military construction and civil works functions. CEFMS is a menu-driven database designed to provide both real-time and batch processing capabilities. CEFMS is the number one systems priority for USACE and failure to provide this system would impair USACE capabilities to effectively manage its major business processes including construction, engineering, and scientific services, as well as its finance and accounting requirements. USACE began development of CEFMS in 1988, and the system was initially deployed in December 1993.

There are 62 separate CEFMS databases operated by users at headquarters, divisions, districts, laboratories, and field activities. The 62 CEFMS databases are processed on four Sun Microsystems 6800 Series servers. The four servers are located at two processing centers managed by the U.S. Army Corps of Engineers Enterprise Infrastructure Services (CEEIS) personnel. The two processing centers are the Central Processing Center, located in Vicksburg, Mississippi, and the Western Processing Center, located in Portland, Oregon. The CEFMS Systems Development and Maintenance Directorate located in Huntsville, Alabama, is responsible for the maintenance and security of CEFMS. The UFC located in

[3] A total of 116 audit recommendations were made for both FY 1999 and FY 2001. The March 2002 GAO report stated that USACE completed 63 of the recommendations with 53 recommendations remaining.

Millington, Tennessee, is responsible for disbursing all of the financial transactions processed in CEFMS.

U.S. Army Corps of Engineers Enterprise Infrastructure Services. The CEEIS wide-area network is critical to the mission of USACE. CEEIS is the data communication backbone that connects USACE headquarters, divisions, districts, and field offices. CEEIS serves approximately 70 division and district locations, and approximately 39,000 users worldwide. CEEIS provides the network infrastructure and server platforms that support USACE personnel in carrying out mission-related functions. CEEIS also provides the transmission paths necessary to support electronic application data for CEFMS, procurement systems, Internet access, and electronic mail. CEEIS consists of routers, firewalls, intrusion detection systems, servers, and the necessary connecting circuits to support the processing needs of USACE. The CEEIS program management office is located at the Central Processing Center.

Objective

Our overall audit objective was to follow up on the Government Accountability Office Report (GAO-02-206), March 2002, and the U.S. Army Audit Agency Report (A-2002-0610-FFC), September 2002, audit recommendations on the U.S. Army Corps of Engineers. Specifically, we determined whether the U.S. Army Corps of Engineers implemented the actions recommended by the Government Accountability Office and U.S. Army Audit Agency. See Appendix A for a discussion of the scope and methodology and prior coverage related to the objectives.

U.S. Army Corps of Engineers Information Assurance

The U.S. Army Corps of Engineers (USACE) had not fully implemented corrective actions recommended by the Government Accountability Office (GAO) and the U.S. Army Audit Agency (AAA). Of the 62 recommendations made by GAO and AAA, USACE had implemented 19, had partially implemented 23, had not implemented 14, and could not implement 2.[4] This condition occurred because USACE had not established an effective Information Assurance (IA) program that included a management-driven remediation plan to ensure that all recommendations were corrected. As a result, USACE continues to have information security vulnerabilities that will persist until management establishes guiding principles for its IA program that comply with Federal laws and DoD and Army Regulations.

Information Assurance

IA is defined as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Organizations need to expect attacks and implement detection tools and procedures that allow them to react to and recover from aggressive actions.

Defense-in-Depth is a practical strategy for achieving IA in highly networked environments. Defense-in-Depth requires a balanced focus on three primary elements: people, technology, and operations. The controls inherent in these elements include: Physical Access Controls, Logical Access Controls, System Software, Application Software Development and Change Control, Segregation of Duties, Network Security, Application Controls, Entity-Wide Security, and Continuity of Operations.

Physical Security Controls

Because GAO did not consistently number all parts of the recommendations, we inserted a letter to clarify that the recommendation contained multiple parts.

GAO-1. Access to Data Center Areas. *Restrict access to the data centers to those employees whose job responsibilities require day-to-day access and periodically review the individuals granted access to ensure that their job responsibilities continue to require this access.*

Not Implemented.

[4] The remaining recommendations will be addressed in a separate report.

USACE Western Processing Center. The CEEIS Western Processing Center (WPC) did not control unauthorized personnel access to restricted areas. AR 380-19 required that an Automated Information System (AIS) security program must prevent unauthorized access to equipment, facilities, material, media, and documents. Management of the proximity card system at WPC allowed unauthorized personnel to access controlled areas. The four access rosters[5] were not fully reviewed and updated. Further, a standard operating procedure did not exist for updating the access rosters and reporting personnel changes to the Portland District Security Office.[6] Finally, the Portland District Security Office did not have an adequate process to ensure that personnel proximity cards only allowed employees access to the areas they were authorized. By reviewing the four access rosters and the access list stored in the proximity card system, we identified the number of individuals with unauthorized access to controlled areas, as shown in Table 1.

Table 1. Number of Individuals with Unauthorized Access to Controlled Areas at the Western Processing Center

Entrance	Number of Individuals
Computer Room	22
System Room	48
Network Operations Security Center	44
West Network Operations Security Center	21

Unauthorized access to controlled areas increases the risk for potential damages to CEEIS functionality. The four controlled areas provide the following functionality to WPC.

- The computer room contains the servers, routers, firewalls, and other support equipment that comprise the WPC portion of the CEEIS network.

- The system room is where system configuration is conducted. The system room also includes the centralized key translation center database that authenticates all of the CEFMS users in the electronic signature system.

[5] The USACE WPC has four areas. Each area has an access roster. The four areas include the Computer Room, the System Room, the Network Operations Security Center, and the West Network Operations Security Center.

[6] The Portland District Security Office is responsible for controlling the proximity card access to the WPC controlled areas.

- The network operations security center is where network monitoring is conducted and computer analysts have the ability to monitor the real-time status of each piece of equipment running at WPC.

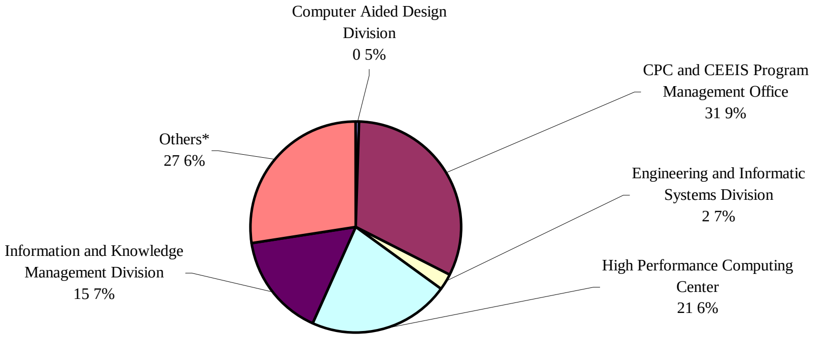
- The west network operations security center was added as a second controlled entrance into the network operations security center.

We randomly selected three individuals that were not listed on the access roster for the system room and network operations security center to determine if they could access the two areas. All of the selected individual’s proximity cards allowed them unauthorized access to the controlled areas. One of the selected individuals stated that he was unaware he had access to the system room. Unauthorized physical access to equipment and computer terminals in controlled areas, such as the system room, increases risks to the operation and availability of the CEEIS network. As a result, unauthorized access to systems, such as the key translation center database, increases risks and decreases confidentiality and trust in the electronic signatures used to authorize documents in CEFMS.

By increasing the risks to the operations of the CEEIS network and allowing unauthorized personnel to access controlled areas, the CEEIS Program Management Office (PMO) did not to achieve the personnel and operation elements for a Defense-in-Depth strategy.

USACE Central Processing Center. The CEEIS PMO and USACE Central Processing Center (CPC) share access to the Joint Computing Facility with nine other organizations. Each organization reviews access to the Joint Computing Facility on a quarterly basis. The 2003 fourth quarter access list identified 185 individuals that had proximity card access to the Joint Computing Facility. However, CEEIS and CPC management are only responsible for 31.9 percent (59 of 185) of the individuals with access to the computing room facility. Chart 1 provides the percentages of cardholders by organization with access to the Joint Computing Facility.

Chart 1. Percentage of Cardholders by Organization with Access to Joint Computing Facility



*Others include the Engineer Research and Development Center Security Office, Information Technology Laboratory Executive Office, Management Integration Office, Shiers (Telephone Contractor), and Hermitic Rush (Heating Contractor)

CPC management had restricted access to the Joint Computing Facility by reviewing the Joint Computing Facility access list and comparing it to personnel job descriptions. Although we did not review the access justifications for the other 9 organizations that are outside the control of CPC, 26 of the 126 individuals from the other organizations had not used their proximity card to access the computer room during the previous quarter, which indicates that these users may not require day-to-day access to the computer room.

The CEEIS risk assessment had not addressed risks associated with sharing their computing area. However, there are inherent risks to the operations and availability of the CEEIS network because equipment and access to computer terminals are vulnerable to unauthorized access. The CEEIS PMO should address the risks associated with unauthorized physical access in the CEEIS risk assessment. Additionally, the CEEIS PMO should implement additional physical security controls to ensure that CEEIS resources are protected against unauthorized access.

GAO-2. Deactivating Access of Departing Personnel. *At WPC and CPC, document, implement, and include specific detail in the current formal personnel termination policies and procedures to ensure that all terminated, separated, and reassigned employees check out with the appropriate offices and that documentation of the checkout is prepared and retained.*

Partially Implemented.

USACE Western Processing Center. The Northwestern Division had a detailed policy and procedures for terminating personnel. WPC, because of its physical location, follows the personnel and security policy established by the USACE Northwestern Division for processing civilian personnel separations. The policy included a clearance form that civilian and contractor personnel must complete prior to their last day of employment.[7] Only one individual had left the organization since the clearance form was updated in May 2003. The individual was processed out in accordance with Northwestern Division policy.

USACE Central Processing Center. The CEEIS Security Plan provided guidance for CPC personnel and security issues, but it did not address contractor personnel or how to process temporary, transferring, or student employees as required by National Institute of Standards and Technology (NIST) Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," September 1996. CEEIS PMO personnel provided the names of seven individuals that had left the organization between January 1, 2003 and October 6, 2003; however, they could not substantiate the completeness of the list. Further, the CEEIS PMO had exit forms for only five of the seven individuals. The CEEIS PMO should maintain a comprehensive list of personnel that leave CPC to facilitate accountability and physical access controls.

The CEEIS PMO had not adequately controlled user accounts after employees left the organization. For example, instead of deleting the user identification (ID) at

[7] The clearance form was updated in May 2003 to include contractor employees.

the time the employee left, the administrator changed the user's password to allow CEEIS personnel to access the individual's shared folders. In one instance, an individual's account existed 8 months after leaving the organization. Allowing accounts to remain open creates a vulnerability because individuals could use the user ID to obtain unauthorized access. If the password was compromised, an individual could use the account and cause damage. USACE should create and implement policy and procedures for removing files and folders of employees that leave the organization.

Logical Access Controls

GAO-3. Access Request Procedures. *Enforce existing formal policies and procedures for granting logical access to the CEFMS system, and update the access request form to include justification for granting dial-in access.*

Partially Implemented.

The CEEIS PMO used an access request form to grant CPC and WPC personnel logical access to CEFMS servers. The latest version of the access request form included system names, level of access and justification for privileged access. However, we determined that 9 of 94 CPC and WPC personnel did not have access request forms on file. AR 380-19 required that each user only have access to the information to which they are entitled. We determined that access request forms for 22 of 94 CPC and WPC personnel did not have justification for dial-in access. Further, we determined that CPC personnel used three versions of the access request form. One of the forms did not provide for justification for dial-in access. The CEEIS PMO should create a standard access request form. Additionally, the CEEIS PMO should ensure that all CEEIS personnel have an access request form that includes justification for dial-in access.

GAO-4. Automatic Account Termination. *Modify the new formal procedures to include the requirement to document the monthly review of access lists, and enforce this requirement to ensure that all unneeded emergency and temporary access accounts are terminated.*

Partially Implemented.

Western Processing Center. WPC did not provide adequate guidance to document the status of temporary and emergency accounts. The WPC Userid-Password Administration and Security System (U-PASS)[8] administrator's procedures for determining if temporary accounts had expired did not require administrators to document the results of their review. The procedures suggested reviewing the accounts on a weekly or bi-weekly basis, depending on the number of temporary and emergency accounts in U-PASS. The WPC U-PASS administrator had not documented the reviews. A query of the U-PASS database indicated that WPC did not have any temporary or emergency accounts at the time of our site visit.

[8] The U-PASS is an automated system that accomplishes the administration of userids and passwords for the CEEIS network.

Central Processing Center. The CEEIS PMO did not document reviews of temporary and emergency accounts. A CEEIS PMO official provided written procedures used to review temporary and emergency accounts. The procedures stated that the CPC U-PASS administrators are responsible for ensuring that access was removed when no longer required. Although the procedures stated that a monthly review of temporary and emergency accounts should be accomplished to verify that accounts had not been left open, the procedures did not require the administrator to document the results of the review. The CEEIS PMO should document the results of their reviews to provide an audit trail. A query of the U-PASS database indicated that CPC did not have any temporary or emergency accounts at the time of our site visit.

GAO-5. Password Security. *Limit U-PASS administrators' capability for viewing UNIX and dial-in passwords in clear text and eliminate storage of users' passwords in the U-PASS database.*

Not Implemented.

U-PASS administrators had the capability to view passwords in clear text. The CEEIS PMO stated that, by design, U-PASS maintains the capability to view UNIX and dial-in passwords in clear text. AR 380-19 required that passwords be inhibited, overprinted, or otherwise protected from unauthorized observation on terminals and video displays. The CEEIS PMO provided the USACE Chief Information Officer with a business case, which was awaiting approval, for allowing viewable passwords. The business case stated that U-PASS administrators at local sites assist users logging into the system by viewing the clear text password and by identifying if the password was correct. Further, the business case stated that in limited cases, U-PASS administrators may try to log into the system on behalf of the user to verify the validity of the password. However, when a user is unable to access the system, the U-PASS administrator should reset the password before troubleshooting it.

AR 380-19 stated that after creation, passwords will be handled and stored at the level of the most sensitive data contained in the system and passwords will not be shared. The U-PASS administrator or any unauthorized user that viewed a user's password could log onto the system as the user and perform unauthorized actions that expose the system to data confidentiality and integrity risks.

GAO-6. Security Policy Awareness. *(a) In conjunction with the continued use of the Oracle security audit script, document and explain the purpose of common CEFMS features, accounts, and account privileges (system and object). (b) Also, develop a program, based on the information above, to train Database Administrators [DBAs] in CEFMS Oracle security.*

Part (a), which is discussed in this report, was partially implemented. Part (b) of the recommendation will be discussed in the report on the USACE sites.

USACE had not established a training and awareness program for database administrators. AR 380-19 required that all personnel who manage, maintain, or operate automated systems undergo a training and awareness program covering responsibilities and accountability, system data and access controls, and authorized system configuration management requirements.

The CEFMS Systems Development and Maintenance Directorate (CEFMS Development Center) documented and explained the common features of CEFMS in numerous user manuals. The CEFMS User Manual, "General Initiation Procedures," July 17, 2003, describes the common features of CEFMS, such as the electronic signature capability. Additionally, the CEFMS User Manual, "CEFMS Access Controls and Application Roles," December 2, 2002, describes how each role granted in CEFMS affects a user's capability throughout the various functionalities of CEFMS.

GAO-7. Password Strength Controls. *Reiterate the importance of following the Corps' password requirements on sensitive accounts. Change the passwords on those user accounts that have weak passwords to comply with AR 380-19, and monitor compliance with such requirements.*

Implemented.

The CEFMS Development Center issued guidance, February 8, 2001, on password requirements for sensitive accounts. AR 380-19 required that AIS passwords processing sensitive but unclassified[9] information must at a minimum be 8 character strings using the 36 alphabetic-numeric characters. The CEFMS Development Center guidance restated the password requirements from AR 380-19 and outlined the process for transporting the CEFMS database account password from the individual USACE sites to the CEFMS Development Center.[10] The process outlined by the CEFMS Development Center allowed it to monitor compliance with AR 380-19.

The external technical reviewers executed a query that checked for blank or default passwords on CPC and WPC servers that contained Oracle databases. At CPC, the external technical reviewers determined there were no default vendor passwords, blank passwords, or passwords matching usernames. However, at WPC, the external technical reviewers identified two active accounts that had a default username and password. WPC personnel corrected the two accounts. Additionally, the external technical reviewers determined there were default passwords on the WPC databases with default accounts that were locked. The external technical reviewers recommended the deletion of the default accounts or, at a minimum, changing the default password and locking the account. The precautionary measures would help prevent an operating vulnerability if the accounts were to be unlocked.

GAO-8. Management of Oracle User Roles. *(a) Ensure that all CEFMS DBAs use the Oracle security audit script to assist them in identifying cases of weak Oracle user management; (b) through training, increase DBAs' knowledge of*

[9] Examples of sensitive but unclassified information include information dealing with logistics, medical care, and personnel management; Privacy Act data; contractual data; for official use only information; and certain categories of financial data.

[10] The CEFMS Development Center requires the password for the CEFMS database account to maintain the database structure when releasing changes to CEFMS.

Oracle security so that they gain a better understanding of the rationale for assigning Oracle roles and privileges to users and can more easily identify inappropriate assignments. (c) Also, investigate capabilities to strengthen Oracle user management, and (d) implement appropriate processes to identify default, dormant, and other unneeded accounts and (e) to prevent improper configurations of password-protected roles.

Parts (a), (b), and (d) of the recommendation will be discussed in the report on the USACE sites. Parts (c) and (e), which are discussed in this report, were implemented.

The CEFMS Development Center did not have the authority to require USACE site personnel to review the security audit report on a regular basis. However, CEFMS Development Center officials stated that they periodically review the report for the sites to determine whether the site DBAs reviewed the report. AR 380-19 required that audit trails be reviewed for security implications daily, but at a minimum, should be reviewed once per week. Our report on USACE sites will discuss site reviews of security audit reports.

The CEFMS Development Center did not provide Oracle security training for site DBAs. A CEFMS Development Center official stated that the Information Management division at each USACE site was responsible for training for assigned personnel. Our report on USACE sites will discuss Oracle security training provided to DBAs.

The security audit report provided site DBAs with a tool to determine whether default, dormant, and other unneeded accounts existed on the site's CEFMS database. The security audit report covered 14 areas, such as which users were granted the default role, which users were active in CEFMS without an Oracle account, and which users had the DBA role. Our report on USACE sites will discuss the use of security audit reports as tools to strengthen Oracle user management.

The CEFMS Development Center implemented the Access Request Management System[11] (ARMS) to provide management increased control over user roles. Additionally, the CEFMS Development Center implemented role-based security to restrict user's access within CEFMS. Roles are approved and applied in ARMS before being granted to users. Individuals granted the authority to approve and apply roles must have the appropriate CEFMS application roles in conjunction with an electronic signature card to grant user roles.

The CEFMS Development Center submitted a proposal in May 2003 to the USACE Chief Information Officer to establish a consolidated DBA team. The proposal recommended the creation of a small group of DBAs to be located at the CEFMS Development Center where they would perform the duties of site DBAs, including the review of the security audit report. The proposal would increase the integrity of the CEFMS data and provide consistency in the management of all

[11] ARMS provides an automated process to manage requests and approvals for access to the CEFMS application.

CEFMS databases. The USACE Chief Information Officer had not adopted the CEFMS Development Center's recommendation to consolidate and centrally manage all CEFMS databases.

GAO-9. Management of Oracle Privileges and Permissions. *(1) Evaluate the use of PUBLIC database links and change to PRIVATE database links where possible; (2) disallow INSERT, UPDATE, and DELETE privileges granted to PUBLIC on all CEFMS tables; (3) ensure that roles that allow UPDATE to the ACCESS_CONTROL table are granted only to appropriate users.*

Our report on USACE sites will discuss site reviews of public database links; the CEFMS tables with insert, update, and delete privileges; and the access control table portions of the security audit report. A CEFMS Development Center official stated the site DBAs should verify the results of the security audit report to determine whether vulnerabilities exist on the site's CEFMS database.

GAO-10. Access to Oracle Databases. *(a) Evaluate possible design alternatives to limit and control users' direct access to the CEFMS databases; (b) assign, at each site, the responsibility for monitoring the overall security of the database; and develop a formal policy for investigating security events. (c) We also recommend that the Corps implement the version of J-Initiator that is compliant with federal government standards on encryption and (d) control CEFMS database session idle times to adequately secure user sessions during periods of inactivity.*

Parts (a), (c), and (d), which are discussed in this report, were partially implemented. Part b of the recommendation will be discussed in the report on the USACE sites.

AR 380-19 required that safeguards be implemented to ensure that each person having access to an automated system be held accountable for his or her actions on the system and that sensitive but unclassified information be transmitted by secure means.

The CEFMS Development Center implemented role-based security to restrict user access in CEFMS. According to the CEFMS Development Center, the CEFMS role-based security restricted user access according to the user's job duties. Role-based security allowed the CEFMS Development Center to disable certain functions if necessary. The CEFMS Development Center created a user manual that described the roles available to CEFMS users.

A CEFMS Development Center official stated that each of the USACE sites were responsible for creating their own policies to review, monitor, and investigate the security audit report. The CEFMS security audit report guide and AR 380-19 stated that audit trails should be reviewed on a daily basis. On August 12, 2003, USACE Resource Management issued an information paper that provided guidance to districts for reviewing the security audit report on a quarterly basis; which was a contradiction of AR 380-19. This recommendation will be discussed in the report on USACE sites.

The CEFMS Development Center upgraded the CEFMS web servers to allow for 128-bit encryption. A CEFMS Development Center official stated that the current version of Oracle allows USACE to implement a Java Virtual Machine that uses a secure socket layer to achieve a stronger encryption. The secure socket layer allows a Hypertext Transfer Protocol Secure (HTTPS) connection between the client browser and the CEFMS web server. We verified that CEFMS users connect to the CEFMS web server with 128-bit encryption, by connecting to CEFMS over the Internet. The Federal Information Processing Standards Publication 46-3, "Data Encryption Standard (DES)," October 25, 1999, states that the Triple Data Encryption Standard will be the Federal Information Processing Standards approved symmetric encryption algorithm. At a minimum, the Triple Data Encryption Standard is a 128-bit encryption algorithm.

The CEFMS application does not log off after inactivity because certain jobs may take longer to process. However, a CEFMS Development Center official stated the electronic signature application logs off after 30 minutes of idle time to adequately secure user sessions during periods of inactivity. We verified that the electronic signature application logged off a user after 30 minutes of inactivity.

GAO-11. Command Line Access. *Develop and implement an alternative to eliminate the need for CEFMS users to access a standard UNIX shell account.*

Could Not Implement.

USACE documented a business case for the auditors stating why the GAO recommendation had not been implemented. The business case stated that 2 percent of the 32,000 CEFMS users needed to log directly onto the command line to perform the following tasks:

- redirecting output and changing directories,
- running daily processes,
- running district-specific reports and activities, and
- accessing the previous fiscal year databases.

Additionally, the business case stated that the remaining 98 percent of the CEFMS users require user IDs to run CEFMS but do not have to log into the command line directly. Although the business case acknowledged it was technologically possible to establish a restricted shell that would allow minimal commands to be executed, there were known benefits and drawbacks. The restricted shell, or limiting the login capabilities to a small number, would provide a more secure environment. However, USACE determined the process would be too lengthy and too costly. Although the CEFMS Development Center had accepted the risk associated with direct access to the command line, they had not documented the mitigation strategy in the business case or the CEFMS Systems Security Authorization Agreement.

GAO-12. Monitoring Log Files. *Implement and enforce a procedure for periodic monitoring of web server logs.*

Not Implemented.

The CEEIS PMO had never monitored the CPC or WPC web server logs. AR 380-19 required audit trails be reviewed, at a minimum, one time per week. The CEEIS PMO should create and implement policies and procedures for monitoring web server logs.

GAO-13. Protection of Private Data. *Upgrade to 128-bit SSL encryption. Require users to print Privacy Act reports, if needed, from a local printer. Implement a pop-up warning banner to make users aware that they are about to view sensitive data and that it should not be printed unless sent to a local printer, not a network printer.*

Partially Implemented.

The CEFMS Development Center had upgraded the CEFMS web servers to 128-bit encryption. AR 380-19 required that sensitive but unclassified information be transmitted only by secure means. A CEFMS Development Center official stated that the current version of Oracle allows USACE to implement a java virtual machine that uses a secure socket layer to achieve a stronger encryption. A secure socket layer allows a HTTPS connection between the client browser and the CEFMS web server. We verified that CEFMS users connect to the CEFMS web server with 128-bit encryption by connecting to CEFMS over the Internet.

The CEFMS Development Center did not have policy that prohibited personnel from printing Privacy Act information on network printers and had not implemented a pop-up banner to alert users that they were about to view sensitive data. AR 380-19 required that information labeled sensitive but unclassified must be protected to ensure confidentiality, availability, and integrity. We observed a CEFMS user access sensitive data without being alerted about the sensitivity of the information or instructed to use a local printer instead of a network printer. The confidentiality of CEFMS data is at risk each time a user accesses or prints Privacy Act information.

GAO-14. Anonymous FTP on Corps Systems. *Provide information to customers in a secure, controllable manner that eliminates the requirement for anonymous File Transfer Protocol [FTP].*[12]

Not Implemented.

USACE had not implemented a secure and controllable manner for providing information to customers. AR 380-19 required that appropriate safeguards be implemented to detect and minimize unauthorized access and inadvertent modification or destruction of data. The CEEIS System Security Authorization

[12] Anonymous FTP servers allow a remote user to access information without a valid username and password.

Agreement stated that USACE sites are configured with an Internet accessible segment that allows USACE to comply with requirements for providing information to the public. Additionally, the CEEIS PMO stated that FTP provides a way to transmit large files reliably between USACE sites and customers. The CEEIS System Security Authorization Agreement encouraged the use of secure FTP protocols; however, the CEEIS PMO did not require or enforce a requirement for secure FTP communication.

We did not perform an external penetration test on the USACE FTP server. However, the CEEIS PMO stated the FTP servers are located in the Internet accessible segment and do not have access back into the CEEIS network. Additionally, the CEEIS PMO stated USACE users place data on the FTP server using anonymous access, and the controls established on the server prohibit the data from being altered or overwritten. CEEIS personnel remove the contents of the server weekly and clear the server when inappropriate data is contained on the server. By USACE not eliminating the requirement for anonymous FTP, the risk that unauthorized users could gain access to the data stored on the FTP server continues to exist. USACE should implement a secure and controllable manner for providing information to customers that eliminates the need for the anonymous FTP.

GAO-15. Controls on Dial-In Servers. *Ensure that the composition of all dial-in passwords complies with AR 380-19.*

Implemented.

The external technical reviewers reviewed a system file that stores authorized user accounts and determined there were no guest accounts with a default password.

GAO-16. Usernames and Passwords on Corps Routers. *Require users to supply a unique username and password before logging into any routers.*

Implemented.

The external technical reviewers used the Internet Security Systems Internet scanner tool[13] to determine whether USACE routers had blank passwords and whether routers could be affected by any known vulnerabilities. The scan revealed there were no blank passwords or vulnerabilities on the USACE routers.

GAO-17. Sendmail Functions on Corps Servers. *If the mail server is not needed on the hosts, disable the service. If the mail server is needed, configure the server not to accept VRFY and EXPN commands.*[14]

[13] The Internet Security Systems Internet scanner tool is a vulnerability-scanning tool used to scan computers for vulnerabilities on a local-area network and can check for vulnerable services running on a computer, incorrect computer settings, and other conditions that could lead to computer security vulnerabilities.

[14] The VRFY and EXPN commands allow an unauthenticated intruder to verify valid user IDs and the delivery addresses of mail aliases and mailing lists.

Implemented.

AR 380-19 stated that network administrators are responsible for ensuring that all hardware and software components of the network infrastructure are properly configured, and the security features and controls are properly set to the intended level of system operation.

Western Processing Center. WPC configured the non-CEFMS production servers requiring the sendmail service to not accept the VRFY and EXPN commands. We determined there were 10 non-CEFMS production servers at the WPC. None of the 10 production servers allowed the VRFY and EXPN commands to be executed.

Central Processing Center. CPC disabled the sendmail service on the non-CEFMS production servers not requiring this service. Additionally, CPC configured the non-CEFMS production servers requiring the sendmail service to reject the VRFY and EXPN commands. There were 21 non-CEFMS production servers at CPC. Seventeen of the 21 servers did not allow a connection, indicating that the sendmail service was disabled on those servers. The remaining servers allowed permission; however, the VRFY and EXPN commands did not execute on the server.

System Software

GAO-18. Unix System Configuration. *Protect user IDs and passwords that are transmitted over the network from unauthorized access.*

Implemented.

USACE had protected usernames and passwords that were transmitted over the network. We determined that once a CEFMS user accessed the CEFMS Web Page, their network traffic, including their CEFMS user ID and Unix/Oracle passwords were encrypted with 128-bit encryption, in accordance with Federal standards. Additionally, on December 31, 2003, CEEIS disabled the telnet[15] service from CEFMS servers and required users to either use secure shell[16] or a secure website when making a connection to the CEFMS servers. As a result, passwords are being sent over the network in a secure manner.

GAO-19. Windows NT Security Controls. *Disable the ability to make NULL connections to Windows New Technology [NT] servers. If any software relies on NULL connections (such as automated backup software), then upgrade or migrate to software that does not rely on NULL connections before disabling.*

[15] Telnet allows a user to log into a system over a network.

[16] Secure shell allows a user to log into another computer over a network and execute commands on the remote machine. Secure shell provides strong authentication and secure communications over insecure channels and is used as replacement for telnet.

Not Implemented.

USACE did not disable the ability to make null connections to Windows NT servers on the USACE internal network. AR 380-19 required that remotely accessed computer systems and file servers possess features to positively identify users and authenticate their ID before processing. We did not validate whether null connections could be made external to the network because GAO reported that the Windows NT servers only allowed null connections from inside the USACE network. USACE did not migrate the Citrix software operating on Windows NT servers or have an action plan to migrate to software that would not allow null connections. Further, USACE had not assessed or mitigated the risks associated with null connections in the CEEIS risk assessment. The use of null connections exposes USACE to data integrity and confidentiality risks. The CEEIS PMO should document the risks associated with null connections in the CEEIS risk assessment and should document their action plan for mitigating the risks. Additionally, USACE should research technologies that do not rely on null connections.

GAO-20. Unix Security Policies and Procedures. *Develop formal test plans and procedures to verify that critical processing functions operate correctly after a system upgrade. Also, develop and formalize policies and procedures for the maintenance of an installation log that will list all currently authorized software for each host.*

Implemented.

The USACE CPC and WPC maintained a checklist for testing systems in order to verify that critical processing functions were operating correctly after an upgrade had been implemented. Additionally, CPC and WPC retained installation logs in electronic spreadsheets to document the server software installations, including all of the CEFMS and UNIX servers.

GAO-21. Use of Generic Accounts. *Review the necessity of generic accounts and remove those that are not necessary. Instruct administrators first to log in using their own individual accounts and then log in to the shared generic account, where possible. In addition, periodically review the appropriate audit logs to identify any suspicious activities involving the generic accounts.*

Partially Implemented.

USACE personnel stated that generic accounts are reviewed on a semi-annual basis. However, we did not verify whether the generic accounts used by USACE were necessary. AR 380-19 required that the knowledge of individual passwords be limited to a minimum number of persons and that passwords not be shared. A CEFMS Development Center official stated that generic accounts are system accounts that are needed to operate CEFMS.

The USACE systems did not force users to log on as themselves before performing the “su” command.[17] The CEEIS special access form instructed

[17] The “su” or switch user command changes the user ID associated with a session.

administrators to first log onto the system using their account and then use the "su" command to log into the generic account when possible. However, the systems did not force users to follow this procedure. The "su" command provides an audit trail for identifying a specific user that accessed the generic account. By not requiring systems to force users to log on as themselves and then use the "su" command, CEEIS will not have the ability to identify individuals that logged onto generic accounts.

The CEEIS personnel use the Log Check program to identify any suspicious activity involving generic accounts. The Log Check program scans the system log files searching for exceptions to a predefined set of criteria and notifies system administrators by e-mail if there are any unusual activities. However, we did not verify how the system administrators processed the e-mail once the Log Check program generated the e-mail.

GAO-22. Unix Server Configuration for the CEFMS Firewalls. *We recommend that the Corps obtain and install the latest security patches on its firewalls; comply with AR 380-19 password policies; construct the PATH variable so that the directory search order is system directories, application directories, and user directories (if needed); and include a secondary nameserver on the CEFMS firewalls. We also recommend that the Corps limit root access to the minimum number of staff necessary to maintain system operations.*

Implemented.

The external technical reviewers determined that the WPC and CPC servers are running Solaris 8 with the most recent kernel[18] patch on their firewalls. Solaris 8 is the most recent Solaris operating system supporting Gauntlet firewalls.
AR 380-19 required system administrators to periodically check with manufacturers, to stay informed of system security problems and patches, and to apply patches in order to maintain automated information systems security.

The external technical reviewers determined that the "/etc/default/passwd" file[19] was in accordance with the AR 380-19 requirement to change passwords semi-annually. The file stated that passwords were only valid for 24 weeks or 168 days, thereby, requiring the passwords to be changed at least twice a year. Additionally, the external technical reviewers determined that CPC and WPC tested the complexity of the passwords by using a password-cracking tool after the passwords were changed.

The external technical reviewers determined that the settings for the default shell path variable were used correctly and were set to the following directory search order: system directories, application directories, and user directories. When a command is entered into a computer, the computer searches through the directories for the command in the order specified by the path variable. Once the command is found, it is executed.

[18] The kernel is the central module of an operating system and is responsible for memory, processes, tasks, and disk management.

[19] The "etc/default/passwd" file sets the parameters for passwords.

The external technical reviewers determined that a secondary Domain Name Server on the CEFMS firewall was not necessary because USACE used Gauntlet as the CEFMS firewalls. GAO reported that the CEFMS firewall was configured with only one Domain Name Server listed in its configuration file. The CEFMS firewall software allowed the entry of only one Domain Name Server in its configuration file. Additionally, the CEFMS firewall software overrode settings in the operating system configuration file. The external technical reviewers determined that the correct Domain Name Server was listed in the Gauntlet configuration file.

The external technical reviewers reviewed the "etc/default/passwd" configuration file and determined that there was only one user ID with root access. AR 380-19 required that each user have access only to the information to which they are entitled and that users be restricted from having access to system privileges that allow operations on data and other system resources not required to perform their job.

Application Software Development and Change Control

GAO-23. Documenting Test Plans and Results. *Document test plans and test results for all recorded CEFMS changes.*

Partially Implemented.

The CEFMS Development Center had standard operating procedures for documenting test results. However, the procedures were not signed or dated. The procedures required programmers to write a summary of the code changes and test results in the findings block located in the Problem Report System[20] after the coding changes were finished. A report from the Problem Report System did not describe the test information in the finding block. However, the final resolution block described the basic test plan and results and did not provide a detailed summary of the tests conducted. The CEFMS Development Center should ensure that test plans and test results are adequately documented to allow users of the Problem Report System to determine test methodology and results.

GAO-24. Web Server Change Management. *Pursuant with the Corps' focus on configuration management, document the procedure and approval process for making changes. Establish a change control committee to coordinate changes, approve changes, or both.*

Partially Implemented.

USACE established the following control and advisory boards:

- Configuration Control Board,
- System Advisory Board,

[20] The Problem Report System is used to submit and track customer inquiries, problem reports, software changes, and test results for CEFMS.

- Network Advisory Board,
- Security Advisory Board, and
- Active Directory Advisory Board.

The Configuration Control Board's mission is to provide decision-making and information technology asset management support to the USACE Chief Information Officer by using the best business practices for configuration management. The mission of the advisory boards is to provide decision-making and information technology asset management support to the CEEIS Program Manager.

The CEEIS PMO finalized the CEEIS Configuration Management Plan (Configuration Plan) on September 3, 2003. The Configuration Plan established the responsibilities and authorities of key personnel, maintenance procedures, and functional and physical configuration audits. The Configuration Plan covers changes to CEEIS, including changes to web servers.

However, the Configuration Plan did not include procedures for emergency changes, Information Assurance Vulnerability Alerts (IAVA), and testing. Additionally, the Configuration Plan did not provide clear guidance on what level of management is required for approving Engineering Change Proposal (ECP). Annex A of the Configuration Plan provided a description of the ECP process. The Configuration Plan stated that the Advisory Boards, CEEIS Program Manager, and Configuration Control Board would review and approve ECPs. However, neither the Configuration Plan nor the ECP process describes or designates the authority or scope for each level of approval. A flow chart of the configuration control process is included in Appendix E.

The Configuration Plan states that if the ECP is within the authority of the approving level, they can approve the ECP or send it to the next level if the ECP is not within their authority. Further, the charters of the control and advisory boards state they could only recommend to the next higher level whether to approve or disapprove an ECP. The CEEIS Configuration Plan and control and advisory charters are not clear on who can approve or disapprove an ECP. As a result, technicians or advisory boards could approve an ECP outside their authority. The CEEIS PMO should clearly define the approval process in the Configuration Plan and the charters for the advisory boards.

GAO-25. Demonstration Files on CEFMS Web Servers. *Remove any Web server content that is not used for production. Relegate sample or demonstration files to development server.*

Implemented.

USACE removed sample or default files and directories from web-servers. The external technical reviewers and audit team used manual and automated processes to review 15 production web-severs at CPC and WPC and determined that the USACE web-servers did not contain sample or default files and directories.

Segregation of Duties

GAO-26. Development Staff Assigned Access to Production Systems. *Explore the possibilities of applying functionality within CEFMS, similar to that which is granted to auditors, to protect data from being inappropriately changed by development staff. An emergency user ID, with appropriate controls, could be employed to provide system level access, when necessary, to support system operations.*

This recommendation will be discussed in our report on USACE sites. USACE officials stated that USACE sites own their CEFMS databases. Therefore, they have the responsibility to assess the compliance and appropriateness of CEFMS access controls.

GAO-27. Segregation of Duties Concept for Information Management Employees. *(a) Implement a procedure whereby current segregation of duties techniques are reviewed to determine that they still provide adequate control. (b) Require management to train employees on segregation of duties concepts to ensure that they understand those actions that are incompatible with their current job duties and responsibilities. (c) Also, periodically review and evaluate job descriptions to document key incompatible duties and identify opportunities for closer supervision or other monitoring activities. (d) Further, review and evaluate ways to segregate the system administrator and database administrator functions and increase the level of supervisory review to control activities until the incompatible duties can be segregated.*

Partially Implemented.

AR 380-19 required that key duties be clearly delineated and separated to reduce the risk of one individual adversely affecting the entire system operation.

The CEEIS PMO developed a segregation of duties policy for WPC on July 1, 2003, and for CPC on February 14, 2003. However, the CEEIS PMO stated that the policy for both sites was under revision. The WPC and CPC segregation of duties policies contained job descriptions and documented key incompatible duties for system administrators, including ways to segregate the system administrator and DBA functions. Additionally, the WPC and CPC policies stated that when an individual's duties may not be segregated, the site managers should document the reasons why access is required. Further, the site managers should plan and implement compensating controls to mitigate the associated risks. For example, the compensating controls for individuals with duties that were incompatible would include logging and monitoring the individual's activities.

USACE provided inadequate segregation of duties training to CPC and WPC personnel. The CPC and WPC policy stated that an annual briefing would be given to personnel to train them on segregation of duties concepts. We observed a training session at WPC conducted by CEEIS PMO personnel. The training did not provide information on the requirements, criteria, and concepts of segregation of duties. The training allowed personnel to review their job descriptions and provide comments if any discrepancies were identified. By not identifying and training personnel on the requirements, criteria, and concepts of segregation of duties, personnel may not be aware of the significance and consequences of performing incompatible duties.

The report on USACE sites will identify whether USACE sites consistently created and implemented policy and trained information management personnel on segregation of duties concepts.

GAO-28. Lead Web Administrators. *Designate a lead web administrator to provide a central focal point for the CEFMS Web servers.*

Implemented.

The CEEIS PMO verbally designated a lead CEFMS web administrator on March 24, 2003. The web administrator will be further designated in the annual review of segregation of duties policy.

GAO-29. Documentation on Web Servers. *Maintain documentation that addresses critical information of CEFMS Web servers, such as software design and capabilities.*

Partially Implemented.

The WPC and CPC personnel maintained a hardware and software baseline that addressed critical information on each of the servers operating at both locations, including the CEFMS web servers. The hardware and software baseline outlined the applications that operate on each of the servers, including the current version of the operating system and database software. However, the WPC and CPC hardware and software baseline did not indicate the capabilities of the operating system, database software, or other software running on the servers. AR 380-19 required that documentation addressing software design and capabilities be maintained for the use of programming, operations, and user personnel.

Network Security

GAO-30. Capturing Security Events. *Implement a logging server on the Finance Center switch and router to capture security events. Also, maintain synchronization of clock settings on the routers and switches.*

Partially Implemented.

The U.S. Army Corps of Engineers Finance Center (UFC) switches and routers are physically located at the UFC in Millington, Tennessee. However, the CEEIS PMO is responsible for the operations and monitoring of routers located at the USACE sites. The UFC is responsible for the operations and monitoring of their own switches.

USACE Finance Center. UFC had not synchronized the clock settings for all of the UFC switches. The UFC defined the use of a network time protocol server operating on the CEEIS network for 15 of the 16 switches. The remaining switch was defined as a back-up time reference source for the UFC switches and would synchronize the clocks of the UFC switches in the event the CEEIS time reference server was not available. However, the UFC back-up time reference source did not maintain a synchronized time with an external source. Therefore, the switch may not contain the correct time, and personnel will have difficulties investigating security incidents when the primary time reference server is not available. UFC should define an external time reference source for the UFC switch that acts as the back-up time reference source.

UFC had implemented a logging server to capture system activity for the switches. UFC implemented the Kiwi Syslog Service Manager version 7.0.2 to record the system activity to include the date, time, priority, origin, and description of the system activity on the switches at UFC.

CEEIS Program Management Office. The CEEIS PMO had implemented a logging server to capture system activity on all of the routers in USACE, including the UFC router. The CEEIS PMO implemented a router log that records activity on UFC and other USACE routers. The router log recorded the date and time of the activity, location of the router activity, and the status of interface changes. Additionally, the CEEIS PMO maintained a synchronized clock setting on all of the USACE routers. The CEEIS PMO implemented two network time protocol servers, a primary and backup network time protocol server, to synchronize the time of all the systems operating on the CEEIS network.

GAO-31. Network Eavesdropping. *Conduct a risk-based evaluation to mitigate the threat of network eavesdropping at the Finance Center.*

Not Implemented.

Finance Center officials stated that they had not yet completed a risk assessment. DoD Manual 8510.1 requires that a risk management review be completed during Phase 3 of the certification and accreditation process and should assess system vulnerabilities with respect to the documented threat, ease of exploitation, potential rewards, and probability of occurrence. Without conducting a risk assessment, the UFC could not ensure that they had taken effective measures to mitigate the threat of network eavesdropping. The UFC should perform a risk-based evaluation to mitigate the threat of network eavesdropping at the UFC in accordance with DoD Manual 8510.1.

GAO-32. Password-Protected Consoles. *Ensure that consoles for switches and routers are password protected.*

Implemented.

USACE Finance Center. The UFC ensured that its console switches were password protected. The UFC had a total of 16 switches, which could be accessed by way of a console port at the UFC. The console port configuration file showed that the switches were password protected.

CEEIS Program Management Office. The CEEIS PMO ensured that the consoles for the CEEIS routers were password protected. The external technical reviewers scanned the CEEIS network and identified 67 CEEIS routers. Of the nine CEEIS routers observed at WPC, one was not password protected. A subsequent test at CPC, determined that all of the CEEIS routers had been password protected, including the router that previously had not been protected. Additionally, one router at CPC contained an unencrypted password that was immediately corrected by CEEIS personnel.

Although all of the consoles for the UFC switches and CEEIS routers were password protected, USACE did not have a process to ensure that console passwords were applied correctly. We identified two routers that were not correctly protected, which the CEEIS PMO corrected. The CEEIS PMO should implement a process to identify and protect its routers.

GAO-33. Segregating Network Services. *Limit site-to-site trust to the Finance Center network.*

Not Implemented.

According to, "CEEIS Security Architecture Description," April 8, 2003, site-to-site trust occurs when the site firewall configurations permit connectivity between the sites production networks. USACE had not limited site-to-site trust to the UFC local-area network and had not performed a risk assessment of network traffic allowed to pass through the firewalls. AR 380-19 required network administrators to ensure that all hardware and software components of the network infrastructure are properly configured, and the security features and controls are properly set to the intended level of system operation. A CEEIS PMO official stated that analysis of the network traffic allowed to pass through the firewall would be performed in FY 2004, when CEEIS deployed new firewalls to the field sites.

GAO-34. Router Access Lists. *Employ the security control capabilities of the routers consistent with overall operation requirements of the network, to enhance multiplayer technical control architecture. Any changes planned for the Corps' network should include a plan for enhancing multiplayer technical capabilities within the network, including security controls implemented in the routers. Also, limit virtual terminal access to the Finance Center router to only those users who need access to perform their job functions.*

Implemented.

The external technical reviewers determined that USACE had employed the security control capabilities of the routers. The USACE routers employed anti-spoofing technologies to verify hostname and Internet Protocol (IP) address. Anti-spoofing measures allow messages only from legitimate internal or external IP addresses to enter the Corps of Engineers network.

Additionally, USACE limited Virtual Terminal (VTY) access to the UFC router from 130,254 IP addresses to 8 IP addresses. The external technical reviewers determined that the eight IP addresses could only be accessed using secure shell, which allows for an encrypted connection from one computer directly to another computer. An encrypted connection with one of the eight systems must be established before being permitted to telnet from one of the allowed systems to the routers.

GAO-35. Password Sharing. *In conjunction with implementing Terminal Access Controller Access Control System [TACACS+]*[21]*, assign individual user IDs and passwords to ensure accountability on the routers.*

Implemented.

USACE assigned individual user IDs and passwords to network administrators in order to ensure that accountability was maintained on the USACE routers. The external technical reviewers determined that USACE had implemented TACACS authentication on all USACE routers. The external technical reviewers determined that USACE assigned user IDs and passwords to the network administrators by reviewing the TACACS server and router files.

GAO-36. CPC Gateway Firewall Traffic. *Factor internal threats into risk assessments as part of network modification and enhancement projects. The risks associated with threats originating from within the Corps should be mitigated using all available network control functions, including firewall and routers, consistent with operational objectives.*

Not Implemented.

USACE had not performed a risk assessment of network traffic allowed to pass through the firewalls. AR 380-19 stated that all risk analyses will evaluate the possible vulnerabilities and the security impact on associated AIS and networks within the area of responsibility. A CEEIS PMO official stated that analyses of the network traffic allowed to pass through the firewall would be performed in FY 2004 when CEEIS deployed new firewalls to the field sites.

GAO-37. Trusted IP Addresses. *Limit the IP addresses to only those users requiring access.*

Implemented.

USACE limited the number of IP addresses with access to the CPC Domain Name Server (DNS) Name Server (NS)1 to only those users requiring access. USACE used the "host.allow" file to control access to NS1. USACE reduced the number of IP addresses permitted to connect to NS1 from 1,033 to 28. USACE required the use of specified protocols. Twenty of the 28 IP addresses were permitted to use secure shell to access NS1 and the remaining 8 IP addresses were permitted to use FTP and other backup related protocols. The CEEIS PMO

[21] The TACACS server is a central authentication server that is responsible for controlling access and maintaining accountability of the user IDs on the routers.

should document the rationale for making this decision in the CEEIS security plan.

GAO-38. Password Aging. *Enable system-enforced password aging on the NS1 DNS.*

Partially Implemented.

The CEEIS PMO had not changed passwords for accounts accessing NS1 domain name server on a 6-month basis. The CEEIS PMO stated that in February 2000, users requiring access to NS1 were added in U-PASS for password administration. The U-PASS system requires that passwords be changed every 24 weeks or 6 months. However, we determined that 19 accounts with access to NS1 had passwords that were older than 6 months. AR 380-19 required that passwords on nonsensitive and sensitive but unclassified systems be changed semiannually.

The passwords for 17 of the 19 accounts had not been changed since February 25, 2003. The CEEIS PMO stated the password change was not performed because it was during the configuration freeze period, which occurred between August and September 2003. The passwords for the remaining two accounts had not been changed since December 6, 2001. The CEEIS PMO stated the passwords for the two accounts had not been changed because of an error in creating their home directories. Additionally, the CEEIS PMO stated that the U-PASS password aging mechanism would disable user accounts that had an expired password, which would prohibit individuals from logging into these accounts. We could not validate whether the password aging mechanism disabled user accounts after the passwords expired because the passwords were changed prior to our completed evaluation of the documentation.

Further, two additional accounts had been manually added to NS1, outside the control of U-PASS. The two accounts were added to NS1 in June and August 2001. The CEEIS PMO stated that the two accounts were not added to U-PASS because of an oversight. A NS1 log file showed that the passwords were changed in February 2003 despite not being included in U-PASS. The CEEIS PMO stated that the two accounts had been added to U-PASS.

Unless passwords are changed periodically, the risk is increased that unchanged passwords could become compromised. The CEEIS PMO should ensure that passwords are changed for privileged accounts on a quarterly basis in accordance with AR 25-2. Additionally, to comply with password policies, the CEEIS PMO should schedule password changes so they do not conflict with configuration freezes.

GAO-39. Warning Banners on Gateway Firewalls. *Install DoD-approved warning banners on the gateway firewalls.*

Could Not Implement.

USACE could not install DoD-approved warning banners on the gateway firewalls because USACE changed the type of gateway firewall from Gauntlet to

CISCO PIX. CISCO PIX firewalls do not support the capability to display warning banners. However, the Department of the Army approved the CISCO PIX firewall for use within the Army. Additionally, USACE had not obtained a waiver for the requirement to display warning banners from the Deputy Chief of Staff for Intelligence, G-2, as required in AR 380-53, "Information Systems Security Monitoring," April 29, 1998. Warning banners are necessary on DoD systems because they alert users that monitoring may be conducted and that unauthorized access to the system is prohibited. Additionally, warning banners aid in the prosecution of individuals who misuse a DoD system.

GAO-40. Permits on the Virtual Terminal Interface. *Limit VTY access to the gateway router to only those users who need access.*

Implemented.

The CEEIS PMO had limited VTY access to the gateway routers and reduced the number of IP addresses permitted to access the VTY interface on the gateway routers from 260,254 to 8. Although USACE had limited VTY access to the gateway routers, USACE had not documented the methodology used to determine the number of IP addresses permitted to access the VTY interface. As a best business practice, USACE should document the rationale of these decisions in the CEEIS security plan.

GAO-41. Access to Critical Operating System Files. *Review and remove full access permission for the Everyone group over all directories and files on the Primary Domain Controller [PDC]* [22] *that do not require that level of access. Limit full access permission to files and directories on the PDC to administrators. Any other directories that require access by nonadministrative or service accounts should be specifically set and configured.*

Implemented.

The UFC had reviewed the full access permissions on files and directories for the "Everyone" group and removed full access permissions for the files and directories that did not require that level of access. We determined that three files on the Windows NT PDC allowed the "Everyone" group to have full control permissions. Two of the three files were for Norton Antivirus software; one file had the default setting assigned by the software manufacturer and the other file was a temporary file that had been removed. The remaining file was needed by the Systems Management Server, which was changed by the UFC to only allow the authenticated users group to read the file. UFC should monitor the file permissions on a quarterly basis to ensure that only authorized users can access a file or directory.

GAO-42. User Rights on the Finance Center NT PDC. *Review powerful privileges assigned to users and groups, and restrict powerful privileges to only those individuals who require that level of access to perform their assigned duties.*

[22] The PDC is a server in the Windows NT network that maintains a directory of user accounts and security information. Also, the PDC authenticates usernames and passwords when users log into the network.

Not Implemented.

The UFC had not restricted powerful privileges for the Windows NT PDC to only those individuals who required access to perform their assigned duties. AR 380-19 required users to be restricted from having access to system privileges that allow operations on data and other system resources not required to perform their job. Twenty-six accounts had full system control on the PDC. Six of the 26 accounts had full control over the Windows NT PDC while being logged in under their own user account and they did not have a separate administrator account. The UFC did not require the administrators and the help desk staff to use two accounts; one for administering the network and one for everyday tasks. The National Security Agency, “Guide to Securing Microsoft Windows NT Networks,” states that administrators should have two accounts: one for administering the network, and one for everyday tasks. Failure to prohibit the UFC administrators and help desk staff from using their administrator IDs to perform everyday tasks creates system vulnerabilities. UFC should restrict the use of administrator accounts to the Windows NT PDC console.

GAO-43. Registry Settings. *Modify the NT PDC registry settings to restrict access.*

Partially Implemented.

The UFC Windows NT PDC registry settings that restrict access had not been adequately modified. AR 380-19 required appropriate safeguards in place to detect and minimize unauthorized access and inadvertent, malicious, or non-malicious modification or destruction of data. Further, the National Security Agency, “Guide to Securing Microsoft Windows NT Networks,” recommends that system administrators perform a full backup of the system, including system registry files. UFC personnel stated that they used a security checklist from the Space and Missile Defense Command to implement the required registry setting changes to the Windows NT PDC. However, registry files had not been backed up before making changes to registry settings. Further, changes to the registry settings had not been documented.

The process UFC followed for making changes to the Windows NT PDC registry settings created system vulnerabilities. The Windows NT PDC may not be adequately secure because the changes made to the registry settings and the values affected by the changes were not documented. The UFC should back up registry files before making changes to the settings and should maintain a log of the changes made to registry settings.

GAO-44. Password Aging and Complexity on NT PDC. *Implement a password policy for the NT PDC consistent with the Corps’ password policy, as defined in AR 380-19.*

Partially Implemented.

UFC had implemented the use of U-PASS to issue and manage UFC local-area network user passwords. The UFC implemented the use of U-PASS in November 2002. The passwords generated in U-PASS contain upper and lowercase alphanumeric characters, as required by AR 380-19. A UFC official stated that the user's local-area network passwords are changed every year during the months of May and November.

The UFC had not implemented U-PASS to issue and manage passwords for the Windows NT PDC administrator accounts. The administrator account passwords must be manually changed according to the account settings on the USACE Windows NT PDC. Three administrator accounts had their passwords set to never expire. One of the administrator accounts was disabled because it was no longer needed. Another account was used to install software on the clients' systems; however, the UFC was uncertain if the account was still needed. Administrators used the remaining account for numerous backup agents and backup jobs. An increased risk exists that these administrative accounts could be compromised because they are not being properly changed. The UFC should ensure that passwords for all Windows NT PDC accounts, including administrator accounts, are changed on a regular basis, as required by current regulation.

GAO-45. Built-in Administrator Account. *Rename and restrict the built-in administrator account to the NT PDC system console to prevent this account from being compromised and accessed over the Corps' network.*

Not Implemented.

The UFC had not adequately renamed the Windows NT PDC administrator account. AR 380-19 required appropriate safeguards to be implemented to detect and minimize unauthorized access. UFC renamed the administrator account from "administrator" to an account name that could be easily identified as the administrator account. There is an increased risk that an attacker could easily identify and compromise the renamed Windows NT PDC administrator account. The UFC should rename and restrict the administrator account to the Window NT PDC console to prevent the account from being compromised and accessed over the USACE network.

GAO-46. Warning Banner on NT. *Ensure that systems have appropriate logon banners enabled.*

Implemented.

The UFC ensured that its systems displayed the appropriate logon banners. UFC complied with AR 380-53 and placed a warning banner on the Windows NT PDC. The warning banner notified system users that their activity was being monitored and warned that unauthorized access and misuse of the system were prohibited.

GAO-47. Audit Logs and Policy Settings. *(a) Set the logs so that they cannot be overwritten and ensure that the logs are of sufficient size to minimize potential overflow. (b) Also, develop a program to audit inappropriate user activity.*

Not Implemented.

The UFC had not ensured the Windows NT PDC audit logs were set so they could not be overwritten. AR 380-19 required audit logs be maintained at the server level in a client-server environment and be used to provide a documented history of the AISs use. The Windows NT PDC application, security, and system audit logs could be overwritten once the audit logs reached their full capacity. The UFC had developed a script that would copy the audit logs to a separate file when the event logs reached 5,000 records. However, the script only copied the security logs. The system and application logs remained vulnerable to be overwritten without maintaining a backup file. There is an increased risk that a potential attacker could flood the system with activities to overflow the log files, which would cause the audit logs to be overwritten losing critical logs and audit trails. The UFC should set the Windows NT PDC audit logs so that they cannot be overwritten and re-examine the backup script to ensure copies of the application, security, and system audit logs are being stored.

Further, the UFC had not ensured that the Windows NT PDC audit logs were set to a sufficient size to minimize potential overflow. The UFC set the application audit log file to .5 megabytes, the security audit log file to 1 megabyte, and the system audit log file to 50 megabytes. The UFC log file size is less than the National Security Agency recommended audit log settings. The National Security Agency, “Guide to Securing Microsoft Windows NT Networks,” provided an acceptable size for Windows NT PDC application, security, and system audit logs. The guide recommends the audit logs files be set to 4 gigabytes to prevent the system from halting if the audit logs exceed specified log space. The UFC should perform an assessment of the PDC to determine whether the size of the audit logs is acceptable.

Finally, the UFC had not developed a program to audit inappropriate user activity. AR 380-19 required that audit logs be reviewed for security implications daily but, at a minimum, be reviewed once per week. A UFC official stated the network staff manually reviewed the Windows NT PDC audit logs on a daily basis; however, the UFC had not developed a procedure for documenting the activities the network staff should look for when reviewing the audit logs. The UFC should develop a procedure for reviewing the audit logs.

We reviewed the process USACE sites used to configure and review audit logs. The results will be presented in our report covering USACE sites.

GAO-48. Vulnerability Services on the PDC. *Install the latest patched version of Internet Information Service [IIS] on a server that is not performing authentication functions. De-install all unnecessary services from the PDC, including IIS.*

Partially Implemented.

UFC installed IIS version 5.0 on a server that was not performing authentication functions. However, we could not validate that UFC corrected all the vulnerabilities associated with Internet Information Service 5.0 because we identified weaknesses in the USACE Headquarters process for validating whether

IAVA vulnerabilities were corrected. UFC had installed Internet Information Service version 5.0 on a Microsoft Windows 2000 server, and it was not running on the UFC Windows NT PDC or Backup Domain Controller. Additionally, UFC removed unnecessary services from the Windows NT PDC, such as FTP, Simple Mail Transfer Protocol, and the World Wide Web Publishing Services.

UFC officials had documentation from the Compliance Reporting Database stating UFC corrected the only IAVA issued for Internet Information Service 5.0 during 2003. However, we could not validate whether UFC corrected all vulnerabilities associated with Internet Information Service 5.0 because the Compliance Reporting Databases were unreliable. For example, some districts and divisions reported compliance even though vulnerabilities still existed.

Application Controls

GAO-AC1. Access Authorizations and Recertifications. *(a) Assess compliance with CEFMS access control policies for granting initial system access and for ensuring the continued appropriateness of access at all CEFMS user locations. (b) Work with site information system security officers to improve compliance wherever shortcomings are identified and periodically check to ensure that compliance is consistently maintained.*

This recommendation will be discussed in our report covering USACE sites. USACE officials stated that USACE sites own their CEFMS databases. Therefore, they have the responsibility to assess the compliance and appropriateness of CEFMS access controls.

GAO-AC2. CEFMS Segregation of Duties Controls. *(a) Perform header record testing on critical transactions on a periodic basis to help ensure that incompatible duties are not performed. (b) Remove all unnecessary CEFMS access from all site databases (c) including the assignment of access permissions that enable Huntsville Development Center personnel to generate invoices at other locations. (d) Remove disbursing capabilities from all CEFMS users who do not perform disbursing functions.*

This recommendation will be discussed in our report covering USACE sites. USACE officials stated that USACE sites own their CEFMS databases. Therefore, they have the responsibility to monitor segregation of duties.

GAO-AC3. Subsequent Reviews of Transactions. *Perform post payment audits of critical user transactions processes on disbursing terminals at the Millington Finance Center.*

Implemented.

UFC internal auditors/evaluators conducted post payment audits on commercial transactions. A UFC official stated that evaluators planned to review more than 380 transactions completed from April 2002 to March 2003. UFC issued two interim reports that identified only administrative errors, but no errors in payments for April and May 2002 transactions. UFC should continue to conduct post payment audits on commercial transactions processed at the UFC.

GAO-AC4. E-Signature Personnel Identification Numbers. *Continue working with the Army to resolve the use of NIST standards in lieu of Army password requirements for Electronic Signature [ESIG] Personnel Identification Numbers [PINs].*

Implemented.

The USACE e-signature personnel ID number required a two-factor authentication, password and token, which conforms to the NIST requirements and exceeded the Department of Army's requirements. On November 20, 2003, after two requests for the status of the waiver, USACE obtained a memorandum from the Department of Army that stated the e-signature card did not need a waiver from AR 380-19.

GAO-AC5. CEFMS User Manuals. *Monitor CEFMS development activities to ensure that appropriate attention continues to be focused on keeping CEFMS manuals and related documentation current, whether maintained in paper form or on-line.*

Partially Implemented.

The CEFMS Development Center established a standard operating procedure for reviewing and updating CEFMS user manuals on October 22, 2002. Subsequently, the CEFMS Development Center hired a contractor to assist in the review and update of CEFMS user manuals. AR 380-19 required that documentation addressing software design and capabilities must be maintained. Although a majority (38 of 62) of the manuals had been reviewed within the past 3 years, 31 percent (19 of 62) of the manuals were more than 3 years old. Two of the CEFMS user manuals "Budget and Estimating" and "Interfaces" were more than 9 years old, and the "Frequently Asked Questions" section had not been updated since June 10, 1998.

CEFMS security controls are at risk, and users could potentially perform inadequate or improper procedures because user manuals do not reflect new requirements or the changes to CEFMS. The CEFMS Development Center should ensure that user manuals are updated and reviewed on an annual basis to reflect the current operating status of CEFMS and reflect policy and procedures.

Entity-Wide Security

Because AAA did not consistently number all parts of the recommendations, we inserted a letter to clarify that the recommendation contained multiple parts.

AAA-1. Information Assurance. *(a) Clearly assign information assurance as a full-time responsibility at each Corps site and (b) develop an upward reporting mechanism to monitor the status of information assurance throughout the Corps.*

(c) Ensure that site commanders and major program directors develop and implement security plans for each Corps site and automated information system.

Partially Implemented.

Information Assurance Managers. USACE Headquarters had developed a policy requiring that IA be assigned as a full-time responsibility at each USACE site. A USACE Headquarters official stated they are in the process of assigning the responsibility of IA to full-time positions at each of the USACE sites. An IA memorandum, dated August 1, 2003, tasked commanders at all levels with the responsibility for IA. USACE should ensure that all USACE sites assign IA as a full-time responsibility.

Information Assurance Reporting Mechanism. USACE Headquarters had not adequately developed an upward reporting mechanism to monitor the status of IA throughout USACE. USACE Headquarters developed an IA website that provides USACE personnel with IA resources and information for IA processes; such as IAVA policies, training resources, and recommendations for securing a system. Additionally, USACE Headquarters developed an upward reporting mechanism to monitor IA throughout USACE by using the Army Knowledge Online Compliance Reporting Database. However, the database did not allow USACE to adequately report IAVA compliance. A USACE Headquarters official stated that a new version of the database, although launched in November 2003, was not fully operational. USACE personnel had to generate reports manually through e-mail, starting at the districts and reporting up the chain of command to the Department of the Army Chief Information Officer to ensure IAVAs were completed. USACE should develop efficient and reliable procedures for handling, tracking, and reporting IAVA messages.

Security Plans. USACE Headquarters had not ensured that each USACE site had developed and implemented adequate security plans for each network and AIS. USACE issued an IA Policy Memorandum on January 10, 2001, that required commanders and designated approving authorities[23] (DAAs) to ensure that networks and AISs had an IA Plan that includes:

- a description of the system;
- assessments and audits;
- personnel security, training, and security measures and procedures to include emergency access procedures;
- incident response;
- continuity; and
- improvements in relation to accreditation requirements.

[23] The DAA is an official with the authority to formally assume responsibility for operating a system at an acceptable level of risk

USACE did not require the network and AIS security plans to include sections on the rules of the system and system interconnection, as required by Office of Management and Budget Circular A-130, Appendix III. Additionally, USACE had not provided the audit team with the status of network and AIS security plans. USACE Headquarters did not have an adequate process in place to track and review network and AIS security plans. USACE will be unable to create an adequate overall security plan until network and AIS security plans are properly completed. USACE Headquarters should ensure the completion of network and AIS security plans that include all sections required by Office of Management and Budget Circular A-130 Appendix III, and implement a standard process for tracking and reviewing security plans.

The report on USACE sites will identify whether the USACE sites had created and implemented adequate network security plans.

AAA-2. Quality Assurance Program. *Develop and implement a quality assurance program to monitor the effectiveness of entity-wide security management and service continuity controls throughout the Corps.*

Partially Implemented.

USACE Headquarters had not properly developed and implemented a consistent process for maintaining a quality assurance program. The Department of the Army issued a memorandum to USACE regarding IAVA on February 26, 2001. The memorandum stated there had been numerous reports of malicious activity directed against the USACE network and systems resulting in unauthorized access. Further, the memorandum stated that vulnerability scans of the USACE network and systems identified that vulnerabilities still existed after USACE had reported IAVA messages complete.

USACE Headquarters issued the following plans, policies, and guidance for monitoring the effectiveness of entity-wide security management and service continuity controls:

- IA Memorandum, August 2003;
- Security Executive Summary, August 2002;
- Short-Range IA Plan Instructions, April 2001; and
- IA Policy Statement, January 2001.

The four documents discuss how USACE will determine their entity-wide security posture. However, it is not clear which requirements USACE personnel should follow. The IA Memorandum requires that all USACE computer assets be scanned for vulnerabilities at a minimum of once a year, while the Security Executive Summary states that USACE servers and sites will be scanned for vulnerabilities every 6 months. Further, the documents are not clear whether USACE Districts’ or USACE Headquarters’ IA personnel are responsible for conducting the audits and assessments. Because the USACE requirements for vulnerability scanning are not clear, USACE Districts may not identify and correct system security vulnerabilities, thereby, increasing the risk of compromise.

USACE Headquarters should develop and implement consistent policies and procedures for maintaining a quality assurance program throughout USACE. The policy should clearly assign responsibility for conducting, tracking, and following up on vulnerability scans.

AAA-3. Incident Response Capability. *Formalize the incident response capability to include developing a charter that defines the scope of responsibilities and the method for meeting them, and that establishes a policy for reviewing computer security incidents to identify risks and threats. It should also include completing an incident response handbook.*

Partially Implemented.

The CEEIS System Security Authorization Agreement Appendix K, "Incident Response Plan," dated October 1, 2003, stated that the purpose of the incident response plan (that is incident response charter) is to ensure that all security incidents or violations are investigated, documented, and reported to appropriate authorities. Appendix K includes the Incident Response Policy and appendices containing forms and procedures for reporting security incidents. However, the incident response plan did not include the virus reporting form or the security incident form.

A USACE official stated that USACE Headquarters had worked with CEEIS personnel to create an incident response package (that is incident response handbook). The incident response package included three standard operating procedures, including the:

- CEEIS Incident Response Plan,
- CEEIS Incident Response (First Steps Guide), and
- CEEIS Incident Response for Worm-Related Events.

The procedures act as a guide for System Administrators and CEEIS personnel on uniform incident handling. Additionally, the procedures provide guidance on who should be contacted and what action should be taken in immediate response situations. However, USACE did not develop the procedures on how the IA Managers should maintain and track the incident log.

AAA-4. DoD Information Technology Certification and Accreditation Process. *(a) Fully implement the DOD Information Technology Security Certification and Accreditation Process for the Corps network and automated information systems to include:*

(b) *Assigning a headquarters employee with responsibility for monitoring Corps-wide accreditation activities.*

(c) *Identifying personnel responsible for accrediting division and district-specific automated information systems.*

(d) *Identifying sufficient accreditation training for designated approving authorities.*

(e) *Updating and completing the Corps-wide risk assessment, security plan, and continuity-of-operations plan.*

Part (a) will be discussed in the report on the USACE Sites. Parts (b) through (e), which are discussed in this report, were partially implemented.

USACE Headquarters appointed two full-time employees with the responsibility of monitoring USACE accreditation activities. Additionally, USACE Headquarters maintained a list of DAAs for USACE divisions, districts, laboratories, and field operating activities. The list identified that 85 percent of the sites had a DAA.

USACE identified and provided sufficient accreditation training for DAAs. However, USACE Headquarters did not track whether the DAAs had received accreditation training. The Assistant Secretary of Defense for Networks and Information Integration policy memorandum, "DoD Information Assurance/Information Technology Designated Approving Authority Training and Certification Requirements," July 15, 2003, requires that all DAAs complete a basic web-based training course and maintain a signed course completion certificate in their personnel file. USACE Headquarters was unable to provide the auditors with a list of DAAs that had completed the required training. USACE Headquarters should develop a consolidated list of DAAs and other personnel who require DAA training, ensure that DAAs complete the required training prior to accrediting a system or network, and document training in personnel records.

The CEEIS PMO completed a risk assessment, security plan, and Continuity of Operations Plan (COOP) for the CEEIS network. However, the CEEIS PMO did not update them to reflect system and network changes that have occurred since they were finalized.

Our review of whether the USACE sites completed a DoD Information Technology Security Certification and Accreditation Process for their networks will be presented in a separate report.

AAA-5. Personnel Security Investigations. *Appoint a manager at the headquarters level to plan, coordinate, monitor, and report on the progress of completing background investigations. Ensure that background investigations for all personnel in automated data processing positions are timely, complete, and fully documented.*

Not Implemented.

Although USACE Headquarters had assigned a Command Security Manager, the USACE Security Manager did not ensure that personnel security investigations were completed. The USACE Security Manager had not tracked the status of security investigations since May 2002; after the Department of the Army requirement for submitting updates was cancelled. After May 2002, USACE site security managers were responsible for tracking security investigations. DoD Regulation 5200.2, "Personnel Security Program," dated January 1987, requires the heads of DoD Components to establish and maintain a program designed to evaluate the security eligibility of their personnel on a continuing basis.

USACE had not prioritized, focused, or regulated personnel security investigations to ensure that personnel in sensitive positions were properly investigated. IG DoD Report No. D-2003-134, "System Security of the Army Corps of Engineers Financial Management System," September 15, 2003, recommended that USACE evaluate the automated data processing levels for DoD and contractor personnel and require them to obtain the correct security investigations before assuming job duties. On February 11, 2004, the USACE Chief Information Officer agreed to evaluate the automated data processing levels for DoD and contractor personnel and require them to obtain the correct security investigations.

AAA-6. Physical Security Reviews. *Conduct periodic reviews to ensure all Corps sites implement physical access controls over computer rooms, workstations, and personal computers.*

This recommendation will be discussed in our report covering USACE sites. USACE Headquarters officials stated that command staff inspections of USACE sites are performed at the USACE Division level and not at the headquarters level.

Continuity of Operations

AAA-7. Continuity of Operations Plan. *(a)Update the continuity of operations plan for the Corps of Engineers Enterprise Information System to document steps needed to restore network operations. (b)Coordinate with program manager for all Corps sites and major automated information systems to ensure they complete and integrate continuity of operations plans for all Corps sites and major automated information systems with the network plan.*[24]

Part (a), which is discussed in this report, was partially implemented.

The CEEIS PMO updated and finalized the CEEIS COOP on January 31, 2003. However, the CEEIS COOP had not integrated COOPs for all USACE sites and major AISs. A CEEIS official stated that they were working with the sites to obtain their respective COOPs. Additionally, CEEIS officials requested that the Corps of Engineers Corporate Information (CECI) Directorate provide them with

[24] Part (b) will be discussed in the report on the USACE sites.

a list of AISs critical to their operation. However, USACE Headquarters officials stated that a list of AISs would not be completed until June 2005 because USACE is waiting on the completion of COOPs for the USACE networks and AISs. Without a complete list of critical systems, USACE could not make an informed decision of which systems are critical to their mission in the event of a COOP situation. USACE should aggressively continue to work toward completing and integrating a COOP for all USACE sites and major AISs.

Our review of whether the USACE sites had created and updated their COOPs will be presented in a separate report.

AAA-8. Continuity of Operations Plan Testing. *Periodically test the continuity of operations plans for the network, Corps sites, and major automated information systems using integrated scenarios and adjust the plan as necessary to correct critical weaknesses.*

Not Implemented.

The CEEIS PMO has not adequately tested the network COOP. Additionally, the COOP had not been adjusted to correct identified critical weaknesses. The CEEIS PMO provided documentation on what they considered operational tests. The tests were for redundant circuits and system notifications, which are real life operational failures. However, the operational failures and notifications were not periodically tested and were not integrated in scenarios with the network, USACE sites, and major AISs. Additionally, the CEEIS COOP had not been adjusted as necessary to correct critical weaknesses because integrated tests with the network, USACE sites, and major AISs were not completed.

USACE should periodically test the CEEIS COOP by using integrated scenarios with the network, USACE sites, and major AISs. Additionally, the CEEIS PMO should make adjustments to the Continuity of Operations Plan after conducting tests to ensure that critical weaknesses are corrected.

We reviewed the process USACE sites used to test their COOP; the results will be presented in our report covering USACE sites.

AAA-9. Backup Facility Risk Assessment. *Conduct a risk assessment to determine what a sufficient distance between primary processing facilities and off-site storage facilities would be to keep backup tapes for the Corps of Engineers Financial Management System.*

Partially Implemented.

The CEEIS Program Management Office provided an assessment of, “The CEEIS Offsite Backup and Archival Facilities,” dated September 30, 2003. The assessment addressed factors for providing emergency services to all sites in the event that normal services were disrupted. The assessment states that CPC and WPC maintained a local backup storage area within approximately 5 to 10 minutes of the facilities to ensure recovery from local, partial system disruptions. The Defense Information System Agency Instruction 360-225-08, “Information Services,” stated the prevailing standard within the disaster recovery industry is a minimum of 25 miles between each site. The CEEIS assessment did not address the risk that the primary processing facilities and off-site storage facilities are physically too close to one another and could be affected by the same natural disaster.

Strategy of Implementing Recommendations

USACE had not established an effective IA program that included a management-driven remediation plan to ensure that all recommendations were corrected. A remediation plan is a critical document for documenting and tracking the implementation of the audit recommendations. DoD Directive 7650.3, "Followup on General Accounting Office, DoD Inspector General, and Internal Audit Reports," February 14, 1992, states that followup is an integral part of good management. DoD Directive 7650.3 requires management to maintain records of actions and time schedules for responding to and acting on findings and recommendations. Additionally, AR 36-2, "Audit Reports and Followup," April 26, 1991, requires internal review to maintain a system for tracking the implementation of corrective actions until fully completed and to include a complete record of actions taken on report recommendations.

Further, USACE Headquarters had not provided the GAO audit report to the UFC and CEFMS Development Center with the associated guidance and support to ensure that the recommendations were implemented. USACE should develop and implement a management-driven remediation plan to ensure that all audit recommendations are properly implemented. Additionally, USACE should develop a process that provides all USACE operating locations, including the processing centers, Finance Center, and CEFMS Development Center with copies of audit reports discussing information assurance vulnerabilities.

Impact of Non-Implemented Recommendations

USACE will continue to have information security vulnerabilities until management establishes the guiding principles of its IA program that complies with Federal laws and DoD and Army Regulations. USACE had partially implemented 23 and had not implemented 13 of the GAO and AAA recommendations. Defense-in-Depth requires a balanced focus on three primary elements: people, technology, and operations. However, the CEEIS PMO, UFC, and USACE Headquarters had not properly implemented all the elements of the Defense-in-Depth strategy.

The CEEIS WPC allowed unauthorized personnel to access controlled areas, which increased risks to the operations and availability of the CEEIS network. CEEIS also permitted U-PASS administrators to view users passwords, which could allow unauthorized users to perform actions that expose the systems to issues of data confidentiality and integrity. CEEIS had not assessed or mitigated the risks associated with null connections that could also expose systems to issues of data integrity and confidentiality.

UFC had not restricted powerful privileges for the Windows NT PDC. Six of the 26 accounts with powerful privileges had full control over the Windows NT PDC while being logged in under their own user accounts. UFC had not

ensured the Windows NT PDC audit logs were properly set, increasing the risk that a potential attacker could flood the system with activities to overflow the log files.

Finally, the USACE Resource Management at Headquarters provided guidance to Districts for reviewing the security audit report that directly contradicted AR 380-19 and guidance established by the CEFMS Development Center. Requirements for conducting vulnerability scanning were not clear. USACE Districts may not identify and correct security vulnerabilities to their systems, which increases the risk that USACE systems could be compromised.

Recommendations, Management Comments, and Audit Response

1. We recommend that the U.S. Army Corps of Engineers Director of Corporate Information:

a. Develop and implement a management-driven remediation plan, in accordance with DoD Directive 7650.3, to ensure that all audit recommendations are properly implemented.

Management Comments. USACE concurred and stated that a management-driven action plan would be developed and implemented by January 31, 2005.

b. Develop a process that provides all U.S. Army Corps of Engineers operating locations, including the U.S. Army Corps of Engineers Enterprise Infrastructure Services processing centers, Finance Center, and U.S. Army Corps of Engineers Financial Management System Systems Development Center with copies of audit reports discussing information assurance vulnerabilities.

Management Comments. USACE concurred and stated that a collaborative tool, as part of the 2012 reorganization, will be purchased and deployed by January 31, 2005. The tool will provide all USACE operating locations with copies of audit reports discussing information assurance vulnerabilities.

c. Implement a secure and controllable manner for providing information to customers that eliminates the need for the anonymous File Transfer Protocol.

Management Comments. USACE nonconcurred and stated that it has court-mandated requirements to provide information to its partners, customers, and the public. Providing the information by way of anonymous FTP allows information to be transferred regardless of format and is more efficient for moving large files.

USACE enforces the following safeguards and controls on its anonymous FTP servers:

- The FTP severs are located on the CEEIS Internet Accessible Segments. The segment is secure and is designed to protect the CEEIS network from intrusion.
- Files are moved from an upload directory to an incoming folder to ensure the integrity of the posted data.
- The FTP server content is automatically and completely deleted every 7 days.
- Users are notified against posting any type of non-public content.
- Activities on the FTP server are logged, and daily messages are sent to the system administrators.

Audit Response. Although USACE nonconcurred with the recommendation, actions taken by USACE to ensure that information is provided to its customers in a secure and controllable manner satisfy the intent of the recommendation. No further comments are required.

d. Research technologies that do not rely on null connections.

Management Comments. USACE concurred and stated that they are currently upgrading to Active Directory. Further, USACE stated that the CEEIS PMO would conduct testing to determine the necessity of null connections for an authentication mechanism within Microsoft products by June 30, 2005. Additional research of other technologies capable of providing the same functionality as null connections will be conducted by June 30, 2005, if null connections are found to be necessary.

e. Assign an individual at all U.S. Army Corps of Engineers sites with the full-time responsibility for the information assurance function.

Management Comments. USACE concurred and stated that a policy was implemented on April 1, 1999. The current policy requires each division and district to appoint an Information Assurance Manager in accordance with Army Regulation.

f. Develop policies and procedures for handling, tracking, and reporting information assurance vulnerability alerts.

Management Comments. USACE concurred and stated that they are currently using the Army Compliance Reporting Database, in accordance with Army Regulation, for handling, tracking, and reporting Information Assurance

Vulnerability Alerts. USACE policy is being updated to reflect the Information Assurance Vulnerability Management policy. The policy is scheduled to be completed in April 2005.

g. Complete a security plan for all U.S. Army Corps of Engineers networks and automated information systems in accordance with the Office of Management and Budget Circular A-130, Appendix III.

Management Comments. USACE concurred and stated that they will update the security plan in accordance with AR 25-2 and Office of Management and Budget (OMB) Circular A-130, Appendix III, by February 15, 2005.

h. Implement a standard process for tracking and reviewing security plans.

Management Comments. USACE concurred and stated that they are in the process of developing a database to track all certifications and accreditations (C&A) to include security plans.

i. Develop and implement consistent policies and procedures for maintaining a quality assurance program throughout U.S. Army Corps of Engineers, including tracking and following up on results of vulnerability scans to ensure vulnerabilities are corrected in a timely manner.

Management Comments. USACE concurred and stated that they will develop and implement consistent policies and procedures for maintaining a quality assurance program throughout USACE by January 31, 2005.

j. Develop a consolidated list of designated approving authorities and other personnel who require designated approving authority training.

Management Comments. USACE concurred and stated that a DAA list had been developed and updated each time the Division and/or District commanders or other DAAs change. USACE stated that the recommended action was completed in June 2002.

Audit Response. Although USACE concurred, the USACE comments are not responsive. A consolidated list of DAAs will not track the completion of training by the DAAs and other personnel who require DAA training. Therefore, we request that USACE inform the Office of the Inspector General DoD when the list will be completed and provide an electronic copy of the completed list of DAAs and other personnel who have completed the required DAA training.

k. Direct designated approving authorities to complete the required designated approving authority training prior to accrediting a system or network and document the completion of training in personnel files.

Management Comments. USACE concurred and stated that they had directed the DAA training both by policy letter and through the command consolidated guidance document. Further, USACE stated that training certificates would be placed in the designated approving authorities' personnel files by December 31, 2004.

l. Complete and integrate a continuity of operations plans for all U.S. Army Corps of Engineers sites and major automated information systems.

Management Comments. USACE concurred and stated that all continuity of operations plans will be completed as part of the C&A process. The completed plans will be reviewed by the Information Assurance C&A team. USACE estimated the completion date to be January 31, 2005.

Audit Response. Although USACE concurred, the USACE comments are partially responsive. The intent of the recommendation was not for USACE to complete individual continuity of operations plans, but for USACE to complete one integrated continuity of operations plan for all USACE sites and major automated information systems. We request that USACE provide additional comments on the final report.

m. Test the U.S. Army Corps of Engineers Enterprise Infrastructure Services Continuity of Operations Plan on a periodic basis by using integrated scenarios with the network, U.S. Army Corps of Engineers sites, and major automated information systems.

Management Comments. USACE concurred and stated that annual testing would be completed on all networks and major AIS. At a minimum, a checklist test will be conducted. USACE stated that the testing would begin by March 1, 2005.

2. We recommend that the U.S. Army Corps of Engineers Enterprise Infrastructure Services Program Management Office:

a. Address the risks associated with unauthorized physical access in the U.S. Army Corps of Engineers Enterprise Infrastructure Services risk assessment.

Management Comments. USACE concurred and stated that the risk assessment would be updated to include authorized access to the joint computing facility tenants by June 30, 2005.

b. Implement physical security controls to ensure that U.S. Army Corps of Engineers Enterprise Infrastructure Services resources are protected against unauthorized access.

Management Comments. USACE concurred and stated that additional physical security controls would be implemented at the CEEIS processing centers; including:

- installing a new key card entry system at CPC,

- requiring the WPC Site Manager to review and authorize all access to the WPC computing facility, an

- conducting a feasibility study of moving the WPC computing facility to a separate facility.

Audit Response. Although USACE concurred, we consider the comments partially responsive. The IG DoD did not intend for USACE to relocate the WPC computing facility to a separate facility. The WPC did not have a standard operating procedure for updating the access rosters and reporting personnel changes to the Portland District Security Office. The Portland District Security Office is responsible for controlling proximity card access to WPC controlled areas. Therefore, the WPC Site Manager must coordinate reviews and personnel changes with the Portland District Security Office. We request that USACE provide comments on the final report identifying the actions the WPC Site Manager will take to control access to the WPC computing facility.

c. Maintain a comprehensive list of personnel that leave the U.S. Army Corps of Engineers Enterprise Infrastructure Services.

Management Comments. USACE concurred and stated that the CEEIS Processing Center IASOs would maintain a list of personnel that leave CEEIS. In addition, CEEIS will include updating personnel lists as part of the center quarterly reviews of the computer room access list. USACE stated that the files would be updated by December 31, 2004.

d. Create and implement policy and procedures for removing files and folders of employees that leave the organization.

Management Comments. USACE concurred and stated that CEEIS has updated its Personnel Security and Access Control policy to include more specific safeguards and requirements, and to establish timeframes for revoking access and subsequent deletion of accounts for departing personnel in accordance with NIST guidance. The CEEIS Personnel Security and Access Control Policy provisions will be fully implemented by June 30, 2005.

e. Create a standard access request form for granting access to the U.S. Army Corps of Engineers Enterprise Infrastructure Services systems.

Management Comments. USACE concurred and stated that the Information Assurance Program Manager (IAPM) would coordinate with USACE sites and

CEFMS to implement a standard access form by way of U-PASS by June 30, 2005.

f. Direct all U.S. Army Corps of Engineers Enterprise Infrastructure Services personnel to have an access request form that includes a justification for dial-in access.

Management Comments. USACE concurred and stated that the IAPM would coordinate with USACE sites and CEFMS to implement a standard access form that includes justification for dial-in access by way of U-PASS. CEEIS will complete the standard access forms for all CEEIS personnel by June 30, 2005.

g. Document the results for reviews of temporary and emergency accounts.

Management Comments. USACE concurred and stated that the CEEIS processing center IASOs would document the reviews of temporary and emergency accounts each month. In addition, USACE stated that U-PASS has been modified to automatically revoke access for expired temporary and emergency accounts and to notify the U-PASS administrator by way of email.

h. Create and implement policies and procedures for monitoring web server logs.

Management Comments. USACE concurred and stated that the IAPM would establish a policy by June 30, 2005, which states that each AIS is responsible for reviewing their respective web server logs for suspicious activity. In addition, CEEIS personnel will assist in the development of standard procedures and access control for log files.

i. Document the risks associated with null connections in the U.S. Army Corps of Engineers Enterprise Infrastructure Services risk assessment and document a plan of action for mitigating the risks.

Management Comments. USACE concurred and stated that the CEEIS PMO would research and test disabling or reducing null connection abilities on its Microsoft servers by June 30, 2005.

Audit Response. The USACE comments were not responsive because they do not address updating the CEEIS risk assessment to include the risks associated with null connections or establish a plan of action to mitigate the risks. Therefore, we request that USACE respond to the final report identifying the actions it will take to document and mitigate the risks associated with the continued use of null connections.

j. Define the change approval process in the U.S. Army Corps of Engineers Enterprise Infrastructure Services Configuration Plan and in the charters for the advisory boards.

Management Comments. USACE concurred and agreed to update the CEEIS Configuration Management Plan by June 30, 2005, to further define the change approval process for CEEIS. However, USACE did not agree that the Configuration Control Board Charters are the appropriate documents in which to define the change approval process for CEEIS.

Audit Response. The USACE comments were partially responsive. Although the CEEIS Configuration Plan should outline the change approval process, the charters should provide personnel with a clear understanding of their authority for approving or disapproving an ECP. We request that USACE provide comments on the final report on how they plan to advise board members on their authorities for approving and disapproving ECPs.

k. Maintain comprehensive documentation on software capabilities for all U.S. Army Corps of Engineers web servers.

Management Comments. USACE concurred and stated that CEEIS maintains documentation on operating systems, databases, and other software capabilities in electronic or online format in accordance with the Paperwork Reduction Act and provides access to the documentation to personnel as needed.

l. Implement a process to identify and protect the U.S. Army Corps of Engineers Enterprise Infrastructure Services routers from unauthorized access.

Management Comments. USACE concurred and stated that the CEEIS PMO started using an automated configuration tool to configure all CEEIS managed routers. The automated configuration tool uses commands to set up passwords for all console ports.

m. Address the methodology for limiting the number of Internet Protocol addresses to systems and interfaces in the U.S. Army Corps of Engineers Enterprise Infrastructure Services security plan.

Management Comments. USACE concurred and stated that the CEEIS security plan would be updated by June 30, 2005, to include the methodology for limiting the number of Internet Protocol addresses with access to CEEIS systems.

n. Schedule password changes to avoid conflicts with the configuration freeze period.

Management Comments. USACE concurred and stated that there is no longer a restriction against password changes during the CEEIS configuration freeze. USACE conducted a password change on June 1, 2004, which will keep future password changes from interfering with the CEEIS configuration freeze.

o. Document the rationale of the decisions to limit virtual terminal interface access to the gateway routers in the Corps of Engineers Enterprise Infrastructure Services security plan.

Management Comments. USACE concurred and stated that the CEEIS security plan would be updated by June 30, 2005, to include the gateway router configuration architecture.

p. Adjust the Continuity of Operations Plan after conducting tests to ensure critical weaknesses are corrected.

Management Comments. USACE concurred and stated that CEEIS would update its COOP by June 30, 2005, to reflect information obtained through testing and evaluation, as well as operational conditions that illustrate prudent changes, modifications, and enhancements. In addition, USACE stated that CEEIS would develop a standard operating procedure for updating the COOP.

3. We recommend that the U.S. Army Corps of Engineers Financial Management System Program Management Office:

a. Provide detailed documentation on test plans and test results to allow users of the Problem Report System to determine test methodology and results.

Management Comments. USACE concurred and stated that the Corps of Engineers Finance Center-Systems (CEFC-S) would modify the Problem Report System by August 31, 2004, to add a test plan and results tab that must be completed for every problem report requiring code changes.

b. Update and review the U.S. Army Corps of Engineers Financial Management System user manuals on an annual basis to reflect the current operating status of U.S. Army Corps of Engineers Financial Management System and reflect current policy and procedures.

Management Comments. USACE concurred and stated that CEFC-S had removed all obsolete user manuals and procedures from the CEFMS user manual website. In addition, USACE will review and replace manuals more than 4 years old by June 30, 2005. Further, USACE will review and update remaining manuals on an annual cycle or when major functionality changes are made to the system.

4. We recommend that the Director of the U.S. Army Corps of Engineers Finance Center:

a. Define an external time reference source for the U.S. Army Corps of Engineers Finance Center back-up switch that acts as the back-up time reference source.

Management Comments. USACE concurred and stated that the UFC synchronized the clocks on its switches with the CEEIS time protocol server and implemented a logging server on March 15, 2004.

b. Perform a risk-based evaluation to mitigate the threat of network eavesdropping at the U.S. Army Corps of Engineers Finance Center in accordance with DoD Manual 8510.1.

Management Comments. USACE concurred and stated that the UFC had completed a risk-based evaluation in March 2004.

c. Monitor the primary domain controller file permissions on a quarterly basis to ensure that only authorized users can access a file or directory.

Management Comments. USACE concurred and stated that the UFC has replaced the Windows NT primary domain controller with a Windows 2003 primary domain controller. Further, USACE stated that the file permissions for the Windows 2003 primary domain controller are reviewed on a quarterly basis. USACE completed the recommended action on July 1, 2004.

d. Restrict the use of administrator accounts to the Windows New Technology primary domain controller console.

Management Comments. USACE concurred and stated that the UFC has replaced the Windows NT primary domain controller with a Windows 2003 Active Directory primary domain controller. Further, USACE stated that the administrator accounts are only used to complete administrative duties. USACE completed the recommended action on July 1, 2004.

e. Back up the registry files prior to making changes to the registry settings.

Management Comments. USACE concurred and stated that the UFC performs backups of the registry files prior to changing the registry settings. USACE completed the recommended action in March 2004.

f. Maintain a written log of the changes made to the registry settings to ensure accountability of changes made to the primary domain controller.

Management Comments. USACE concurred and stated that the UFC maintains a written log of the changes to the primary domain controller registry settings. USACE completed the recommended action in March 2004.

g. Change passwords for all primary domain controller accounts, including administrator accounts, in accordance with Army Regulation 25-2.

Management Comments. USACE concurred and stated that the UFC had implemented the recommended action on the Windows 2003 (W2K3) primary domain controller. USACE completed the recommended action on July 1, 2004.

h. Rename and restrict the primary domain controller administrator account to prevent the account from being compromised and accessed over the U.S. Army Corps of Engineers network.

Management Comments. USACE concurred and stated that the UFC had implemented the recommended action on the W2K3 primary domain controller. USACE completed the recommended action on July 1, 2004.

i. Set the primary domain controller audit logs so that they cannot be overwritten.

Management Comments. USACE concurred and stated that the UFC had implemented the recommended action on the W2K3 primary domain controller. USACE completed the recommended action on July 1, 2004.

j. Re-examine the backup script operating on the primary domain controller to ensure that copies of the application, security, and system audit logs are being stored.

Management Comments. USACE concurred and stated that the UFC had implemented the recommended action on the W2K3 primary domain controller. USACE completed the recommended action on July 1, 2004.

k. Perform an assessment of the primary domain controller to determine whether the sizes of the audit logs are acceptable.

Management Comments. USACE concurred and stated that the UFC had increased the size on the W2K3 primary domain controller on July 1, 2004.

l. Develop policies and procedures for reviewing audit logs in accordance with Army Regulation 25-2.

Management Comments. USACE concurred and stated that the UFC would develop and implement policies and procedures for reviewing audit logs by June 30, 2005.

m. Continue to conduct post payment audits on commercial transactions processed at the U.S. Army Corps of Engineers Finance Center.

Management Comments. USACE concurred and stated that the UFC continues to conduct post payment audits on commercial transactions processed at UFC. USACE completed the recommended action on July 1, 2004.

Appendix A. Scope and Methodology

We assessed the USACE implementation of audit recommendations contained in the GAO Report, "Corps of Engineers Making Improvements, But Weaknesses Continue," (GAO-02-206) and the AAA Report, "Corps of Engineers Financial Management System General and Application Controls," (A-2002-0610-FFC). We interviewed personnel at the USACE Headquarters, Washington, D.C.; USACE Central Processing Center, Vicksburg, Mississippi; USACE Western Processing Center, Portland, Oregon; CEFMS Systems Development and Maintenance Directorate, Huntsville, Alabama; and USACE Finance Center, Millington, Tennessee. We evaluated documents pertaining to the following areas: Physical Access Controls, Logical Access Controls, System Software, Application Software Development and Change Control, Segregation of Duties, Network Security, Application Controls, Entity-Wide Security Controls, and Continuity of Operations.

We reviewed the following Federal laws and DoD and Army Regulations:

- "Federal Managers Financial Integrity Act of 1982," September 8, 1982;

- Office of Management and Budget Circular A-123, "Management Accountability and Control," revised June 21, 1995;

- Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources," November 28, 2000;

- National Institute of Standards and Technology Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," September 1996;

- DoD Directive 3020.26, "Continuity of Operations Policy and Planning," May 26, 1995;

- DoD Directive 7650.3, "Followup on General Accounting Office, DoD Inspector General, and Internal Audit Reports," February 14, 1992;

- DoD Directive 8500.1, "Information Assurance," October 24, 2002;

- DoD Directive 5200.2-R, "Department of Defense Personnel Security Program," January 1987;

- DoD Manual 8510.1, "DoD Information Technology Certification and Accreditation Process Application Manual (DITSCAP)," July 31, 2000;

- Army Regulation 36-2, "Audit Reports and Followup," April 26, 1991;

- Army Regulation 380-19, "Information Systems Security," February 27, 1998;

- Army Regulation 380-53, “Information Systems Security Monitoring,” April 29, 1998; and

- Army Regulation 380-67, “Personnel Security Program,” September 9, 1988.

We performed this audit from July 2003 through June 2004 in accordance with generally accepted government auditing standards. We limited our scope and did not evaluate the USACE management control program. We did not evaluate the management control program because USACE recognized a material weakness in computer system controls in the FY 2002 Statement of Assurance. Additionally, we limited our scope because we were unable to test the following areas.

- We did not validate whether null connections could be made external to the network because GAO reported that the Windows NT servers only allowed null connections from inside the USACE network (GAO-19).

- We did not review the requirement to validate the necessity of generic accounts (GAO-21).

- We did not validate the complete audit process for the USACE Log Check program (GAO-21).

- We did not validate whether the password aging mechanism disabled user accounts after the passwords expired because the passwords were changed prior to our completed evaluation of the documentation (GAO-38).

- We did not validate that UFC corrected all the vulnerabilities associated with Internet Information Service 5.0 because we identified weaknesses in the USACE Headquarters process for validating whether IAVA vulnerabilities were corrected (GAO-48).

- We did not validate whether USACE periodically performed header record testing on critical transactions because both USACE and the audit team were uncertain of the intent of the recommendation (GAO-AC2).

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Use of Technical Assistance. We performed this audit with the assistance of technical advisors from two organizations, the Information Operations Vulnerability Assessment Division from the U.S. Army 1st Information Operations Command and the Technical Assessment Division from the IG DoD Audit Followup and Technical Support Directorate. The technical advisors assisted the audit team in completing the following areas logical access controls, system software, application software development and change control, segregation of duties, and network security.

Government Accountability Office High-Risk Area. The Government Accountability Office has identified several high-risk areas in DoD. This report provides coverage of the effective management of information technology investments high-risk area.

Prior Coverage

During the last 5 years, the GAO, IG DoD, and the AAA have issued four reports related to U.S. Army Corps of Engineers Financial Management System and U.S. Army Corps of Engineers Enterprise Infrastructure Services. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted IG DoD reports can be accessed over the Internet at http://www.dodig.osd.mil/audit/reports.

GAO

GAO Report GAO-02-206, "Corps of Engineers Making Improvements, But Weaknesses Continue," March 2002

IG DoD

IG DoD Report No. D-2004-041, "The Security of the Army Corps of Engineers Enterprise Infrastructure Services Wide-Area Network," December 26, 2003

IG DoD Report No. D-2003-134, "System Security of the Army Corps of Engineers Financial Management System," September 15, 2003

Army

AAA Report A-2002-0610-FFC, "Corps of Engineers Financial Management System General and Application Controls," September 30, 2002

Appendix B. Information Security Policy

Federal Managers Financial Integrity Act (FMFIA) of 1982. The Federal Managers Financial Integrity Act of 1982, September 8, 1982, requires ongoing evaluations and reports of the adequacy of the systems of internal accounting and administrative control of each executive agency.

Office of Management and Budget Circular A-123. The Office of Management and Budget Circular A-123, "Management Accountability and Control," revised June 21, 1995, provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls.

Office of Management and Budget Circular A-130, Appendix III. The Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources," November 28, 2000, establishes Government-wide responsibilities for Federal computer security. Office of Management and Budget Circular A-130, Appendix III, requires Federal agencies to adopt a minimum set of management controls to assure that adequate security is provided for all agency information that is collected, processed, stored, or disseminated in general support systems and major applications. Additionally, Federal agencies are required to assign responsibility for security, to develop a security plan, to perform an independent review or audit of security controls, and to authorize, in writing, the use of an application prior to operating and to re-authorize the use of the application at least every 3 years thereafter.

National Institute of Standards and Technology Special Publication 800-14. The National Institute of Standards and Technology Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," September 1996, provides a baseline that organizations can use to establish and review their information technology security programs. Management, internal auditors, users, system developers, and security practioners can use the guideline to gain an understanding of the basic security requirements most information technology systems should contain. The foundation of the baseline is based on generally accepted system security principles and contains common practices that are used in securing information technology systems.

DoD Directive 3020.26. DoD Directive 3020.26, "Continuity of Operations Policy and Planning," May 26, 1995, requires DoD Components to establish a continuity of operations plan to ensure that mission-essential functions continue effectively and without interruption during any national security emergency. DoD Components shall designate alternate headquarters or emergency relocation sites at each command level down to the lowest level necessary to ensure continuity of operations. Additionally, Heads of DoD Components shall ensure that the continuity of operations plans are updated, tested, and validated at least every 2 years.

DoD Directive 8500.1. DoD Directive 8500.1, “Information Assurance,” October 24, 2002, establishes policy and assigns responsibilities to achieve DoD information assurance through a Defense-in-Depth approach that integrates the capabilities of personnel, operations, and technology. DoD Directive 8500.1 mandates the certification and accreditation of all DoD information systems. Additionally, DoD Directive 8500.1 defines information assurance as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

DoD Regulation 5200.2. DoD Directive 5200.2-R, “Department of Defense Personnel Security Program,” January 1987, states that individuals performing work on unclassified automated information systems (including: DoD military, civilian personnel, consultants, and contractors), may be assigned to one of three position sensitivity designations or automated data processing levels and be investigated as follows:

- Automated Data Processing-I: Background Investigation.
- Automated Data Processing -II: Defense National Agency Check plus Written Inquires or National Agency Check plus Written Inquires.
- Automated Data Processing -III: National Agency Check or Entrance National Agency Check.

DoD Manual 8510.1. DoD Manual 8510.1, “DoD Information Technology Certification and Accreditation Process Application Manual (DITSCAP),” July 31, 2000, provides implementation guidance to standardize the certification and accreditation process throughout DoD. DoD Manual 8510.1 provides an introduction to the certification and accreditation process, an overview of the security process, a detailed description of the certification and accreditation phases, and a summary of management roles and responsibilities throughout the certification and accreditation process. The principal purpose of the DITSCAP is to protect and secure the entities comprising the Defense Information Infrastructure.

Army Regulation 380-19. Army Regulation 380-19, “Information Systems Security,” February 27, 1998, prescribes information systems security policy for the protection of classified and sensitive but unclassified information processed, stored, or transmitted over automated information systems.[*]

Army Regulation 380-53. Army Regulation 380-53, “Information Systems Security Monitoring,” April 29, 1998, establishes responsibilities, policy, and procedures for conducting information systems security monitoring within the U.S. Army. The regulation also provides guidance for the U.S. Army elements conducting information systems security monitoring in support of joint and combined operations and activities.

[*] Army Regulation 25-2, “Information Assurance,” November 14, 2003, replaced Army Regulation 380-19.

Army Regulation 380-67. Army Regulation 380-67, “Personnel Security Program,” September 9, 1988, implements DoD Directive 5200.2-R within the Department of the Army. Army Regulation 380-67 requires DoD military, civilian personnel, consultants, and contractors performing work on unclassified automated information systems to be assigned to one of three position sensitivity designations or automated data processing levels.

Appendix C. Acronym List

AAA	U.S. Army Audit Agency
AIS	Automated Information System
AR	Army Regulation
ARMS	Access Request Management System
C&A	Certification and Accreditation
CEEIS	U.S. Army Corps of Engineers Enterprise Infrastructure Services
CEFC-S	Corps of Engineers Finance Center-Systems
CEFMS	U.S. Army Corps of Engineers Financial Management System
COOP	Continuity of Operations Plan
CPC	Central Processing Center
DAA	Designated Approving Authority
DBA	Database Administrator
DES	Data Encryption Standard
DITSCAP	DoD Information Technology Certification and Accreditation Process
DNS	Domain Name Server
ECP	Engineering Change Proposal
FTP	File Transfer Protocol
GAO	Government Accountability Office
HTTPS	Hypertext Transfer Protocol Secure
IA	Information Assurance
IAPM	Information Assurance Program Manager
IASO	Information Assurance Security Officer
IAVA	Information Assurance Vulnerability Alert
ID	Identification
IG DOD	Office of the Inspector General of the Department of Defense
IIS	Internet Information Service
IP	Internet Protocol
NIST	National Institute of Standards and Technology
NS	Name Server
NT	New Technology
OMB	Office of Management and Budget
PDC	Primary Domain Controller
PMO	Program Management Office
TACACS	Terminal Access Controller Access Control System
UFC	U.S. Army Corps of Engineers Finance Center
U-PASS	Userid-Password Administration and Security System
USACE	U.S. Army Corps of Engineers
VTY	Virtual Terminal
WPC	Western Processing Center

Appendix D. Status of Government Accountability Office and U.S. Army Audit Agency Recommendations

Status of the Government Accountability Office and U.S. Army Audit Agency Recommendations						
Recommendation Number	**Issue Area**	**Implemented**	**Not Implemented**	**Partially Implemented**	**Could Not Implement**	**USACE Sites**
Government Accountability Office – General Controls						
GAO – 1	Access to Data Center Area		X			
GAO – 2	Deactivating Access to Departing Personnel			X		
GAO – 3	Access Request Procedures			X		
GAO – 4	Automatic Account Termination			X		
GAO – 5	Password Sharing		X			
GAO – 6	Security Policy Awareness			X		X
GAO – 7	Password Strength Controls	X				
GAO – 8	Management of Oracle User Roles	X				X
GAO – 9	Management of Oracle Privileges and Permissions					X
GAO – 10	Access to Oracle Databases			X		X
GAO – 11	Command Line Access				X	
GAO – 12	Monitoring of Log Files		X			
GAO – 13	Protection of Private Data			X		
GAO – 14	Anonymous FTP on Corps Systems		X			
GAO – 15	Controls on Dial-In Servers	X				
GAO – 16	Usernames and Passwords on Corps Routers	X				
GAO – 17	Sendmail Functions on Corps Servers	X				
GAO – 18	Unix System Configuration	X				
GAO – 19	Windows NT Security Controls		X			
GAO – 20	Unix Security Policies and Procedures	X				
GAO – 21	Use of Generic Accounts			X		
GAO – 22	Unix Server Configuration for CEFMS Firewalls	X				
GAO – 23	Documenting Test Plans and Results			X		
GAO – 24	Web Server Change Management			X		
GAO – 25	Demonstration Files on CEFMS Web Servers	X				
GAO – 26	Development Staff Assigned Access to Production Systems					X
GAO – 27	Segregation of Duties Concepts for Information Management Employees			X		X

Status of the Government Accountability Office and U.S. Army Audit Agency Recommendations- (Cont'd)

Recommendation Number	Issue Area	Implemented	Not Implemented	Partially Implemented	Could Not Implement	USACE Sites
GAO – 28	Lead Web Administrator	X				
GAO – 29	Documentation on Web Servers			X		
GAO – 30	Capturing Security Events			X		
GAO – 31	Network Eavesdropping		X			
GAO – 32	Password Protected Consoles	X				
GAO – 33	Segregating Network Services		X			
GAO – 34	Router Access Lists	X				
GAO – 35	Password Sharing	X				
GAO – 36	CPC Gateway Firewall Traffic		X			
GAO – 37	Trusted IP Addresses	X				
GAO – 38	Password Aging			X		
GAO – 39	Warning Banners on Gateway Firewalls				X	
GAO – 40	Permits on the Virtual Terminal Interface	X				
GAO – 41	Access to Critical Operating System Files	X				
GAO – 42	User Rights on the Finance Center NT PDC		X			
GAO – 43	Registry Settings			X		
GAO – 44	Password Aging and Complexity on NT PDC			X		
GAO – 45	Built-in Administrator Account		X			
GAO – 46	Warning Banners on NT	X				
GAO – 47	Audit Logs and Policy Settings		X			X
GAO – 48	Vulnerable Services on the PDC			X		
Government Accountability Office – Application Controls						
GAO – 1	Access Authorizations and Recertifications					X
GAO – 2	CEFMS Segregation of Duties Controls		*			X
GAO – 3	Subsequent Reviews of Transactions on Disbursing Terminals	X				
GAO – 4	Electronic Signature Personal Identification Numbers	X				
GAO – 5	CEFMS User Manuals			X		
U.S. Army Audit Agency						
AAA – 1	Information Assurance			X		X
AAA – 2	Quality Assurance Program			X		
AAA – 3	Incident Response Capability			X		
AAA – 4	DoD Information Technology Certification and Accreditation Process			X		X
AAA – 5	Personnel Security Investigations		X			
AAA – 6	Physical Security Reviews					X

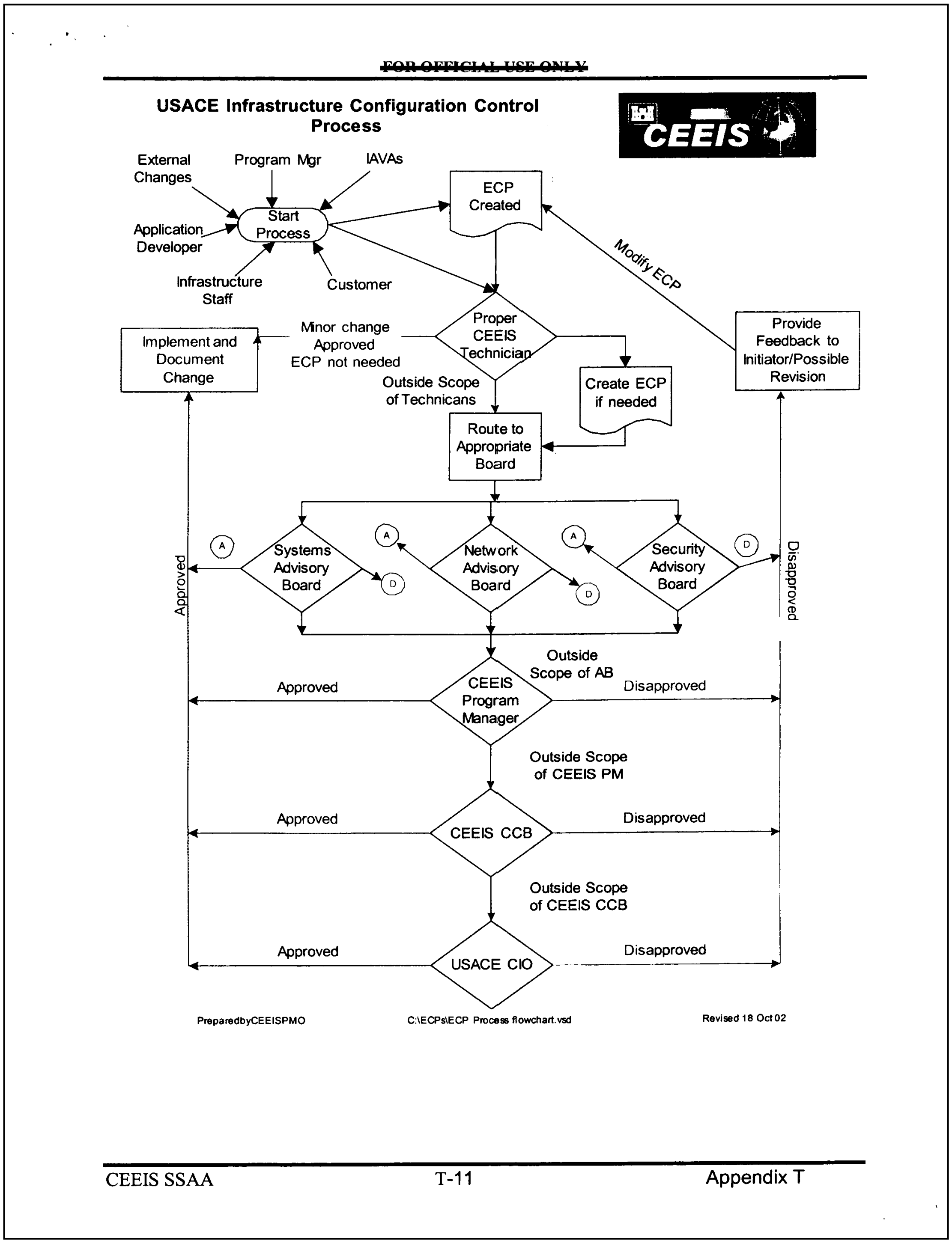
Status of the Government Accountability Office and U.S. Army Audit Agency Recommendations- (Cont'd)

Recommendation Number	Issue Area	Implemented	Not Implemented	Partially Implemented	Could Not Implement	USACE Sites
AAA – 7	Continuity of Operations Plan			X		X
AAA – 8	Continuity of Operations Plan Testing		X			X
AAA – 9	Backup Facility Risk Assessment			X		
	Total	**19**	**14**	**23**	**2**	**14**

Note: Ten of the recommendations are being covered in this report and in our report on USACE sites.
* Could not validate GAO-AC2.

Acronym List:
AAA – U.S. Army Audit Agency
CEFMS – U.S. Army Corps of Engineers Financial Management System
CPC – Central Processing Center
FTP – File Transfer Protocol
GAO – Government Accountability Office
IP – Internet Protocol
NT – New Technology
PDC – Primary Domain Controller

Appendix E. U.S. Army Corps of Engineers Infrastructure Configuration Control Process



~~FOR OFFICIAL USE ONLY~~

USACE Infrastructure Configuration Control Process

PreparedbyCEEISPMO C:\ECPs\ECP Process flowchart.vsd Revised 18 Oct 02

CEEIS SSAA T-11 Appendix T

Appendix F. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)/Chief Financial Officer
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Director, Program Analysis and Evaluation
Assistant Secretary of Defense for Network and Information Integration/Department of Defense Chief Information Officer

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor General, Department of the Army
Chief Information Officer, Department of the Army
Assistant Secretary of the Army (Civil Works)
Commanding General, United States Army Corps of Engineers

Unified Command

Inspector General, U.S. Joint Forces Command

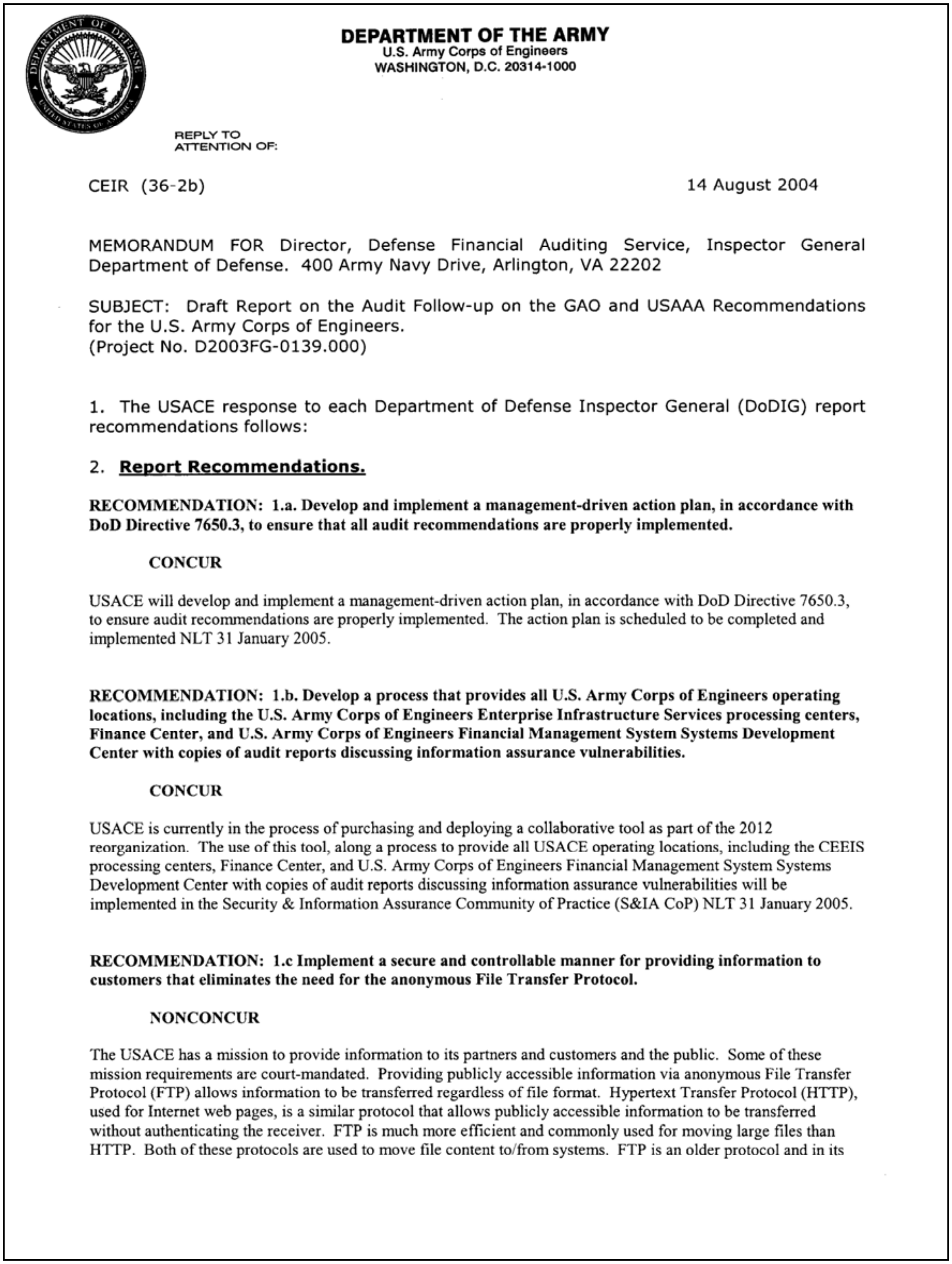
Non-Defense Federal Organization

Office of Management and Budget
Government Accountability Office

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

U.S. Army Corps of Engineers Comments



DEPARTMENT OF THE ARMY
U.S. Army Corps of Engineers
WASHINGTON, D.C. 20314-1000

REPLY TO
ATTENTION OF:

CEIR (36-2b) 14 August 2004

MEMORANDUM FOR Director, Defense Financial Auditing Service, Inspector General Department of Defense. 400 Army Navy Drive, Arlington, VA 22202

SUBJECT: Draft Report on the Audit Follow-up on the GAO and USAAA Recommendations for the U.S. Army Corps of Engineers.
(Project No. D2003FG-0139.000)

1. The USACE response to each Department of Defense Inspector General (DoDIG) report recommendations follows:

2. **Report Recommendations.**

RECOMMENDATION: 1.a. Develop and implement a management-driven action plan, in accordance with DoD Directive 7650.3, to ensure that all audit recommendations are properly implemented.

CONCUR

USACE will develop and implement a management-driven action plan, in accordance with DoD Directive 7650.3, to ensure audit recommendations are properly implemented. The action plan is scheduled to be completed and implemented NLT 31 January 2005.

RECOMMENDATION: 1.b. Develop a process that provides all U.S. Army Corps of Engineers operating locations, including the U.S. Army Corps of Engineers Enterprise Infrastructure Services processing centers, Finance Center, and U.S. Army Corps of Engineers Financial Management System Systems Development Center with copies of audit reports discussing information assurance vulnerabilities.

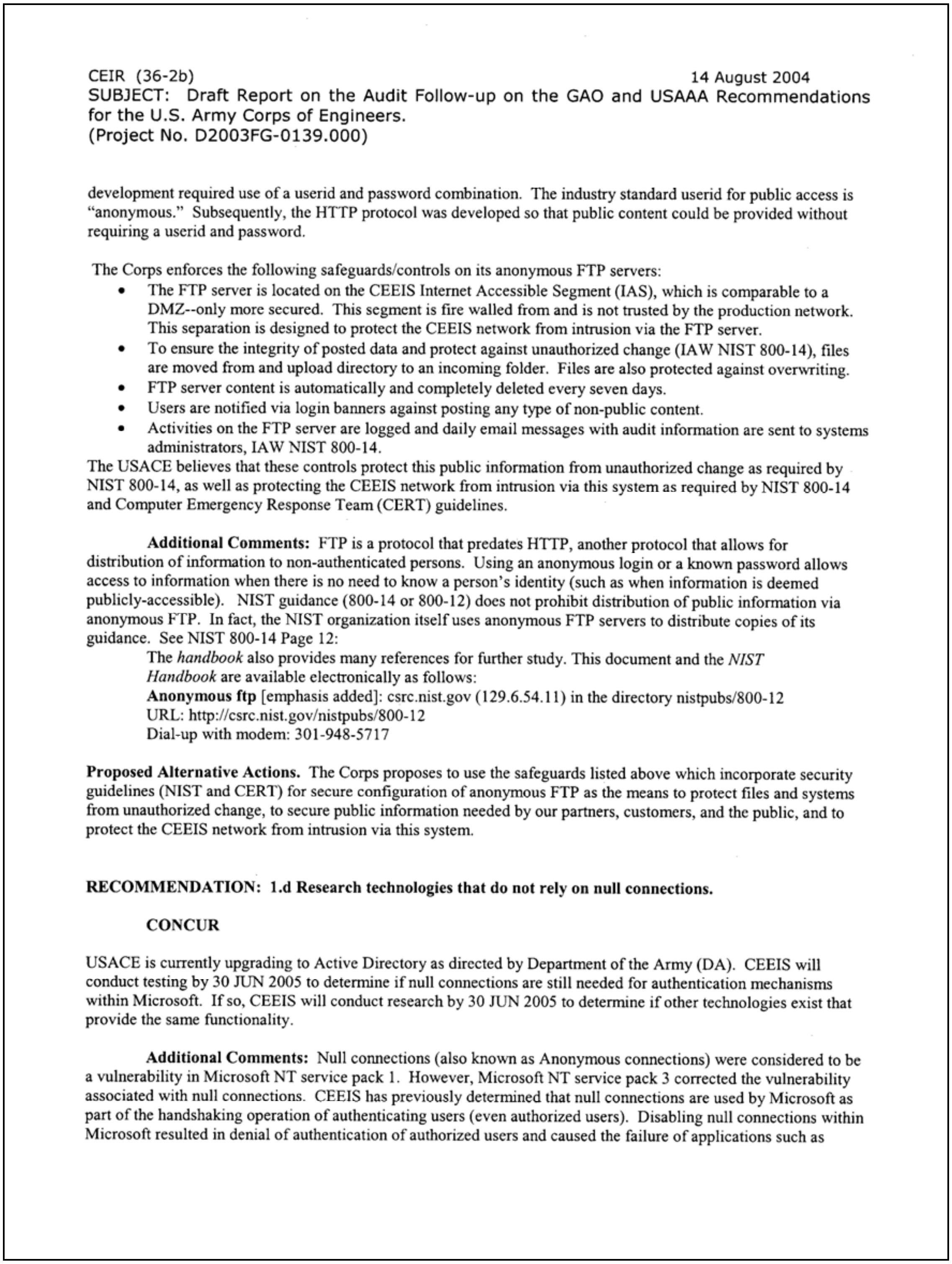
CONCUR

USACE is currently in the process of purchasing and deploying a collaborative tool as part of the 2012 reorganization. The use of this tool, along a process to provide all USACE operating locations, including the CEEIS processing centers, Finance Center, and U.S. Army Corps of Engineers Financial Management System Systems Development Center with copies of audit reports discussing information assurance vulnerabilities will be implemented in the Security & Information Assurance Community of Practice (S&IA CoP) NLT 31 January 2005.

RECOMMENDATION: 1.c Implement a secure and controllable manner for providing information to customers that eliminates the need for the anonymous File Transfer Protocol.

NONCONCUR

The USACE has a mission to provide information to its partners and customers and the public. Some of these mission requirements are court-mandated. Providing publicly accessible information via anonymous File Transfer Protocol (FTP) allows information to be transferred regardless of file format. Hypertext Transfer Protocol (HTTP), used for Internet web pages, is a similar protocol that allows publicly accessible information to be transferred without authenticating the receiver. FTP is much more efficient and commonly used for moving large files than HTTP. Both of these protocols are used to move file content to/from systems. FTP is an older protocol and in its



CEIR (36-2b) 14 August 2004
SUBJECT: Draft Report on the Audit Follow-up on the GAO and USAAA Recommendations for the U.S. Army Corps of Engineers.
(Project No. D2003FG-0139.000)

development required use of a userid and password combination. The industry standard userid for public access is "anonymous." Subsequently, the HTTP protocol was developed so that public content could be provided without requiring a userid and password.

The Corps enforces the following safeguards/controls on its anonymous FTP servers:

- The FTP server is located on the CEEIS Internet Accessible Segment (IAS), which is comparable to a DMZ--only more secured. This segment is fire walled from and is not trusted by the production network. This separation is designed to protect the CEEIS network from intrusion via the FTP server.
- To ensure the integrity of posted data and protect against unauthorized change (IAW NIST 800-14), files are moved from and upload directory to an incoming folder. Files are also protected against overwriting.
- FTP server content is automatically and completely deleted every seven days.
- Users are notified via login banners against posting any type of non-public content.
- Activities on the FTP server are logged and daily email messages with audit information are sent to systems administrators, IAW NIST 800-14.

The USACE believes that these controls protect this public information from unauthorized change as required by NIST 800-14, as well as protecting the CEEIS network from intrusion via this system as required by NIST 800-14 and Computer Emergency Response Team (CERT) guidelines.

Additional Comments: FTP is a protocol that predates HTTP, another protocol that allows for distribution of information to non-authenticated persons. Using an anonymous login or a known password allows access to information when there is no need to know a person's identity (such as when information is deemed publicly-accessible). NIST guidance (800-14 or 800-12) does not prohibit distribution of public information via anonymous FTP. In fact, the NIST organization itself uses anonymous FTP servers to distribute copies of its guidance. See NIST 800-14 Page 12:

> The *handbook* also provides many references for further study. This document and the *NIST Handbook* are available electronically as follows:
> **Anonymous ftp** [emphasis added]: csrc.nist.gov (129.6.54.11) in the directory nistpubs/800-12
> URL: http://csrc.nist.gov/nistpubs/800-12
> Dial-up with modem: 301-948-5717

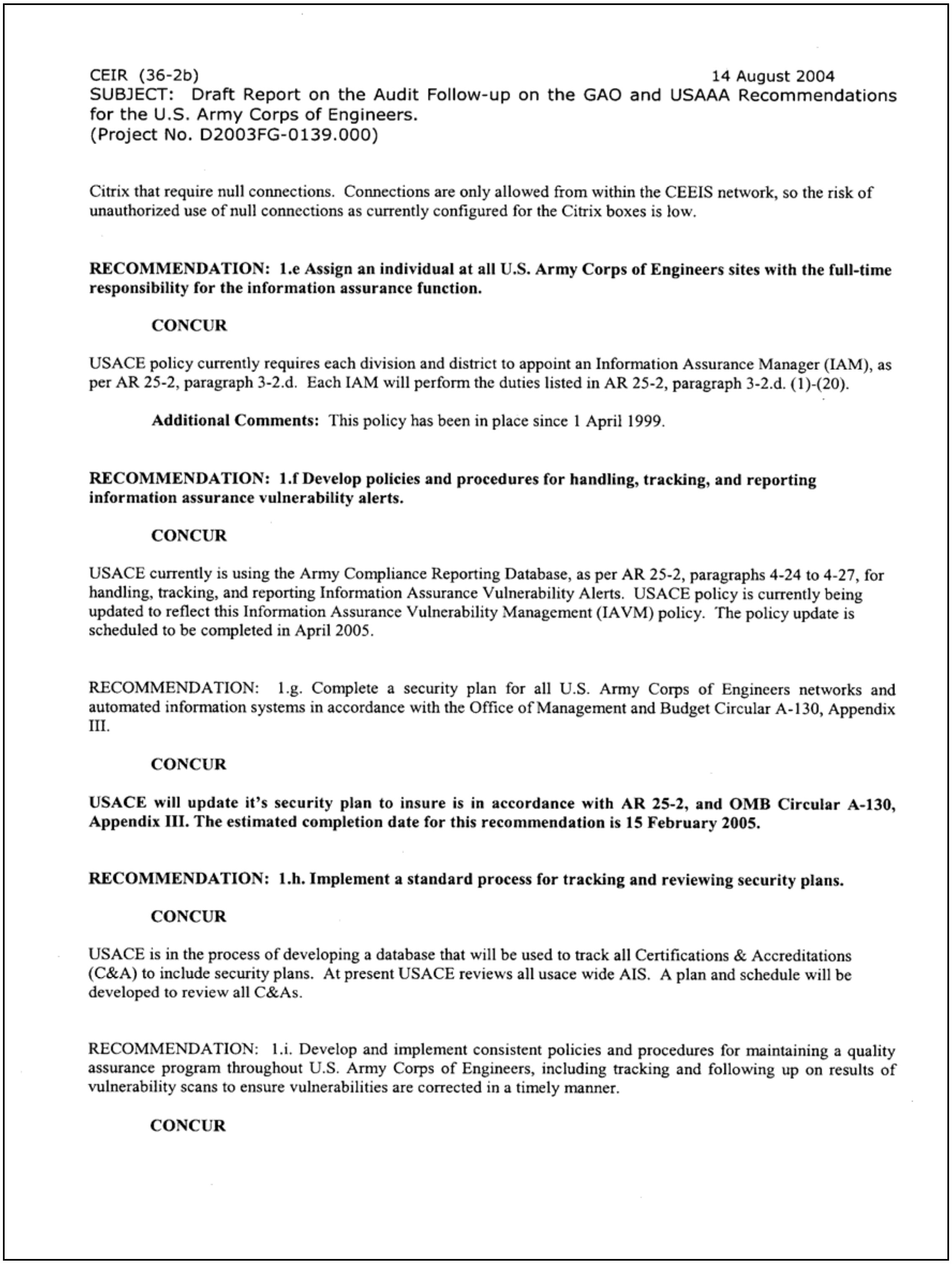
Proposed Alternative Actions. The Corps proposes to use the safeguards listed above which incorporate security guidelines (NIST and CERT) for secure configuration of anonymous FTP as the means to protect files and systems from unauthorized change, to secure public information needed by our partners, customers, and the public, and to protect the CEEIS network from intrusion via this system.

RECOMMENDATION: 1.d Research technologies that do not rely on null connections.

CONCUR

USACE is currently upgrading to Active Directory as directed by Department of the Army (DA). CEEIS will conduct testing by 30 JUN 2005 to determine if null connections are still needed for authentication mechanisms within Microsoft. If so, CEEIS will conduct research by 30 JUN 2005 to determine if other technologies exist that provide the same functionality.

Additional Comments: Null connections (also known as Anonymous connections) were considered to be a vulnerability in Microsoft NT service pack 1. However, Microsoft NT service pack 3 corrected the vulnerability associated with null connections. CEEIS has previously determined that null connections are used by Microsoft as part of the handshaking operation of authenticating users (even authorized users). Disabling null connections within Microsoft resulted in denial of authentication of authorized users and caused the failure of applications such as



CEIR (36-2b) 14 August 2004
SUBJECT: Draft Report on the Audit Follow-up on the GAO and USAAA Recommendations for the U.S. Army Corps of Engineers.
(Project No. D2003FG-0139.000)

Citrix that require null connections. Connections are only allowed from within the CEEIS network, so the risk of unauthorized use of null connections as currently configured for the Citrix boxes is low.

RECOMMENDATION: 1.e Assign an individual at all U.S. Army Corps of Engineers sites with the full-time responsibility for the information assurance function.

CONCUR

USACE policy currently requires each division and district to appoint an Information Assurance Manager (IAM), as per AR 25-2, paragraph 3-2.d. Each IAM will perform the duties listed in AR 25-2, paragraph 3-2.d. (1)-(20).

Additional Comments: This policy has been in place since 1 April 1999.

RECOMMENDATION: 1.f Develop policies and procedures for handling, tracking, and reporting information assurance vulnerability alerts.

CONCUR

USACE currently is using the Army Compliance Reporting Database, as per AR 25-2, paragraphs 4-24 to 4-27, for handling, tracking, and reporting Information Assurance Vulnerability Alerts. USACE policy is currently being updated to reflect this Information Assurance Vulnerability Management (IAVM) policy. The policy update is scheduled to be completed in April 2005.

RECOMMENDATION: 1.g. Complete a security plan for all U.S. Army Corps of Engineers networks and automated information systems in accordance with the Office of Management and Budget Circular A-130, Appendix III.

CONCUR

USACE will update it's security plan to insure is in accordance with AR 25-2, and OMB Circular A-130, Appendix III. The estimated completion date for this recommendation is 15 February 2005.

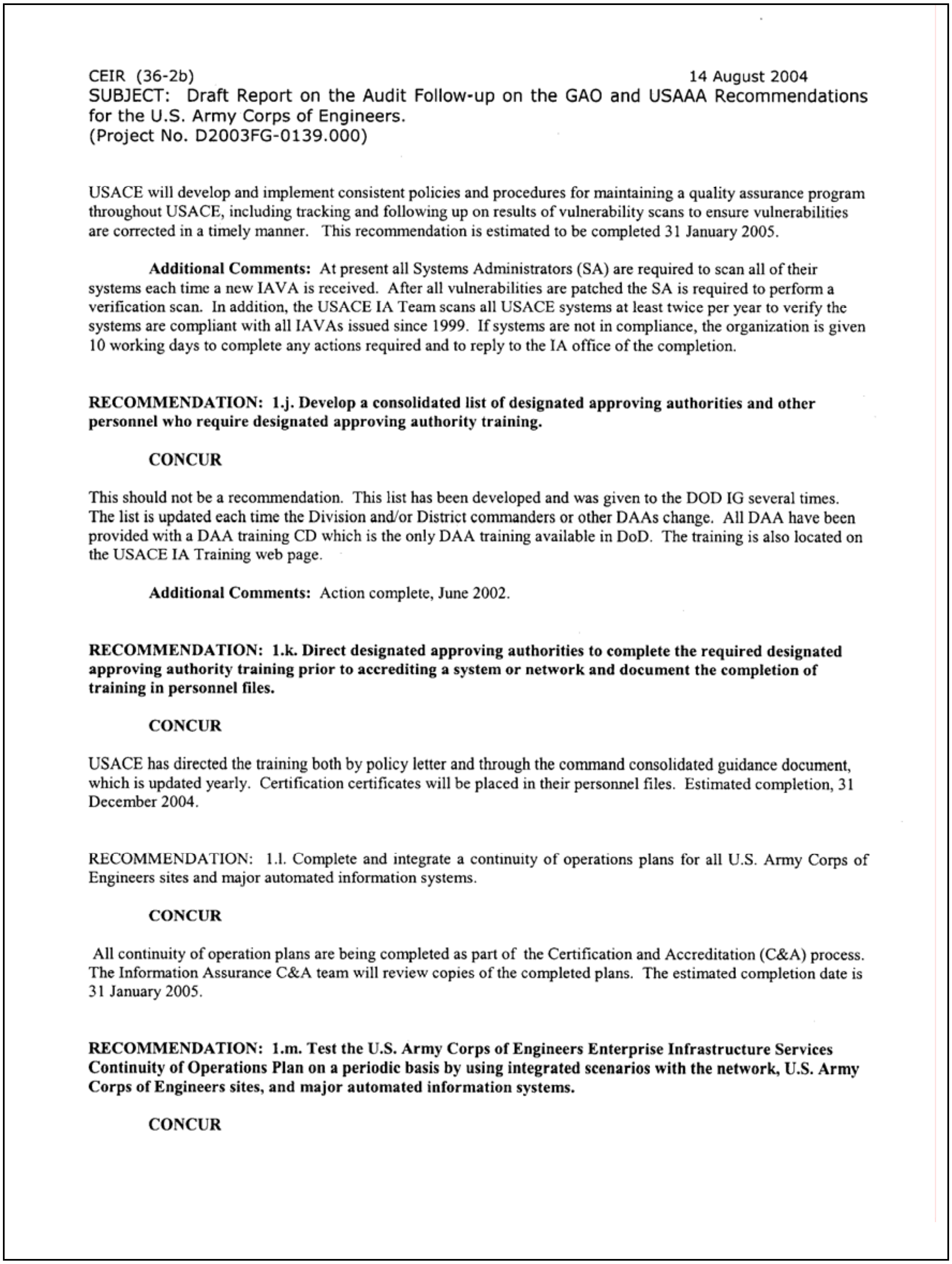
RECOMMENDATION: 1.h. Implement a standard process for tracking and reviewing security plans.

CONCUR

USACE is in the process of developing a database that will be used to track all Certifications & Accreditations (C&A) to include security plans. At present USACE reviews all usace wide AIS. A plan and schedule will be developed to review all C&As.

RECOMMENDATION: 1.i. Develop and implement consistent policies and procedures for maintaining a quality assurance program throughout U.S. Army Corps of Engineers, including tracking and following up on results of vulnerability scans to ensure vulnerabilities are corrected in a timely manner.

CONCUR



CEIR (36-2b) 14 August 2004

SUBJECT: Draft Report on the Audit Follow-up on the GAO and USAAA Recommendations for the U.S. Army Corps of Engineers.
(Project No. D2003FG-0139.000)

USACE will develop and implement consistent policies and procedures for maintaining a quality assurance program throughout USACE, including tracking and following up on results of vulnerability scans to ensure vulnerabilities are corrected in a timely manner. This recommendation is estimated to be completed 31 January 2005.

Additional Comments: At present all Systems Administrators (SA) are required to scan all of their systems each time a new IAVA is received. After all vulnerabilities are patched the SA is required to perform a verification scan. In addition, the USACE IA Team scans all USACE systems at least twice per year to verify the systems are compliant with all IAVAs issued since 1999. If systems are not in compliance, the organization is given 10 working days to complete any actions required and to reply to the IA office of the completion.

RECOMMENDATION: 1.j. Develop a consolidated list of designated approving authorities and other personnel who require designated approving authority training.

CONCUR

This should not be a recommendation. This list has been developed and was given to the DOD IG several times. The list is updated each time the Division and/or District commanders or other DAAs change. All DAA have been provided with a DAA training CD which is the only DAA training available in DoD. The training is also located on the USACE IA Training web page.

Additional Comments: Action complete, June 2002.

RECOMMENDATION: 1.k. Direct designated approving authorities to complete the required designated approving authority training prior to accrediting a system or network and document the completion of training in personnel files.

CONCUR

USACE has directed the training both by policy letter and through the command consolidated guidance document, which is updated yearly. Certification certificates will be placed in their personnel files. Estimated completion, 31 December 2004.

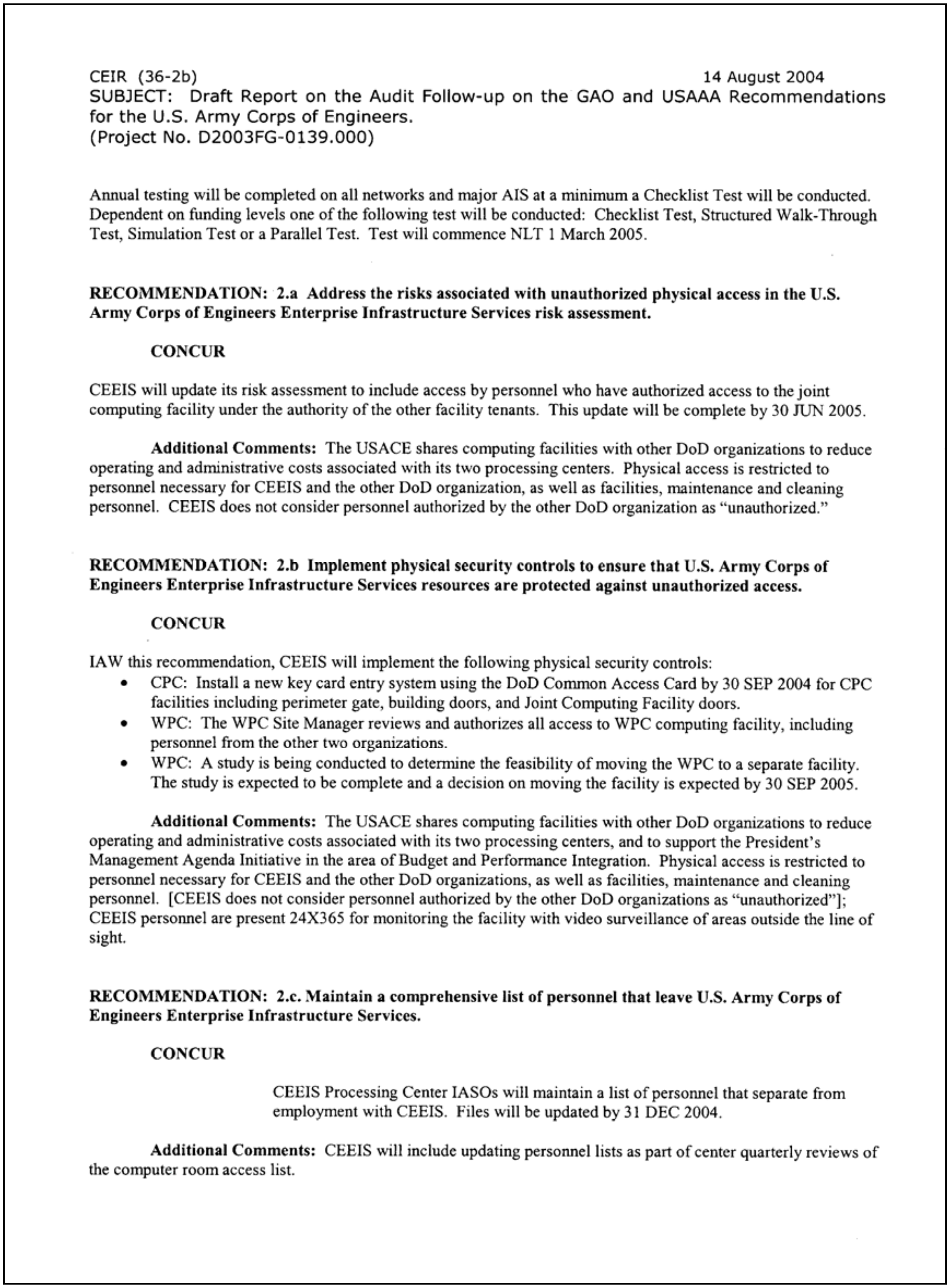
RECOMMENDATION: 1.l. Complete and integrate a continuity of operations plans for all U.S. Army Corps of Engineers sites and major automated information systems.

CONCUR

All continuity of operation plans are being completed as part of the Certification and Accreditation (C&A) process. The Information Assurance C&A team will review copies of the completed plans. The estimated completion date is 31 January 2005.

RECOMMENDATION: 1.m. Test the U.S. Army Corps of Engineers Enterprise Infrastructure Services Continuity of Operations Plan on a periodic basis by using integrated scenarios with the network, U.S. Army Corps of Engineers sites, and major automated information systems.

CONCUR



CEIR (36-2b) 14 August 2004
SUBJECT: Draft Report on the Audit Follow-up on the GAO and USAAA Recommendations for the U.S. Army Corps of Engineers.
(Project No. D2003FG-0139.000)

Annual testing will be completed on all networks and major AIS at a minimum a Checklist Test will be conducted. Dependent on funding levels one of the following test will be conducted: Checklist Test, Structured Walk-Through Test, Simulation Test or a Parallel Test. Test will commence NLT 1 March 2005.

RECOMMENDATION: 2.a Address the risks associated with unauthorized physical access in the U.S. Army Corps of Engineers Enterprise Infrastructure Services risk assessment.

CONCUR

CEEIS will update its risk assessment to include access by personnel who have authorized access to the joint computing facility under the authority of the other facility tenants. This update will be complete by 30 JUN 2005.

Additional Comments: The USACE shares computing facilities with other DoD organizations to reduce operating and administrative costs associated with its two processing centers. Physical access is restricted to personnel necessary for CEEIS and the other DoD organization, as well as facilities, maintenance and cleaning personnel. CEEIS does not consider personnel authorized by the other DoD organization as "unauthorized."

RECOMMENDATION: 2.b Implement physical security controls to ensure that U.S. Army Corps of Engineers Enterprise Infrastructure Services resources are protected against unauthorized access.

CONCUR

IAW this recommendation, CEEIS will implement the following physical security controls:

- CPC: Install a new key card entry system using the DoD Common Access Card by 30 SEP 2004 for CPC facilities including perimeter gate, building doors, and Joint Computing Facility doors.
- WPC: The WPC Site Manager reviews and authorizes all access to WPC computing facility, including personnel from the other two organizations.
- WPC: A study is being conducted to determine the feasibility of moving the WPC to a separate facility. The study is expected to be complete and a decision on moving the facility is expected by 30 SEP 2005.

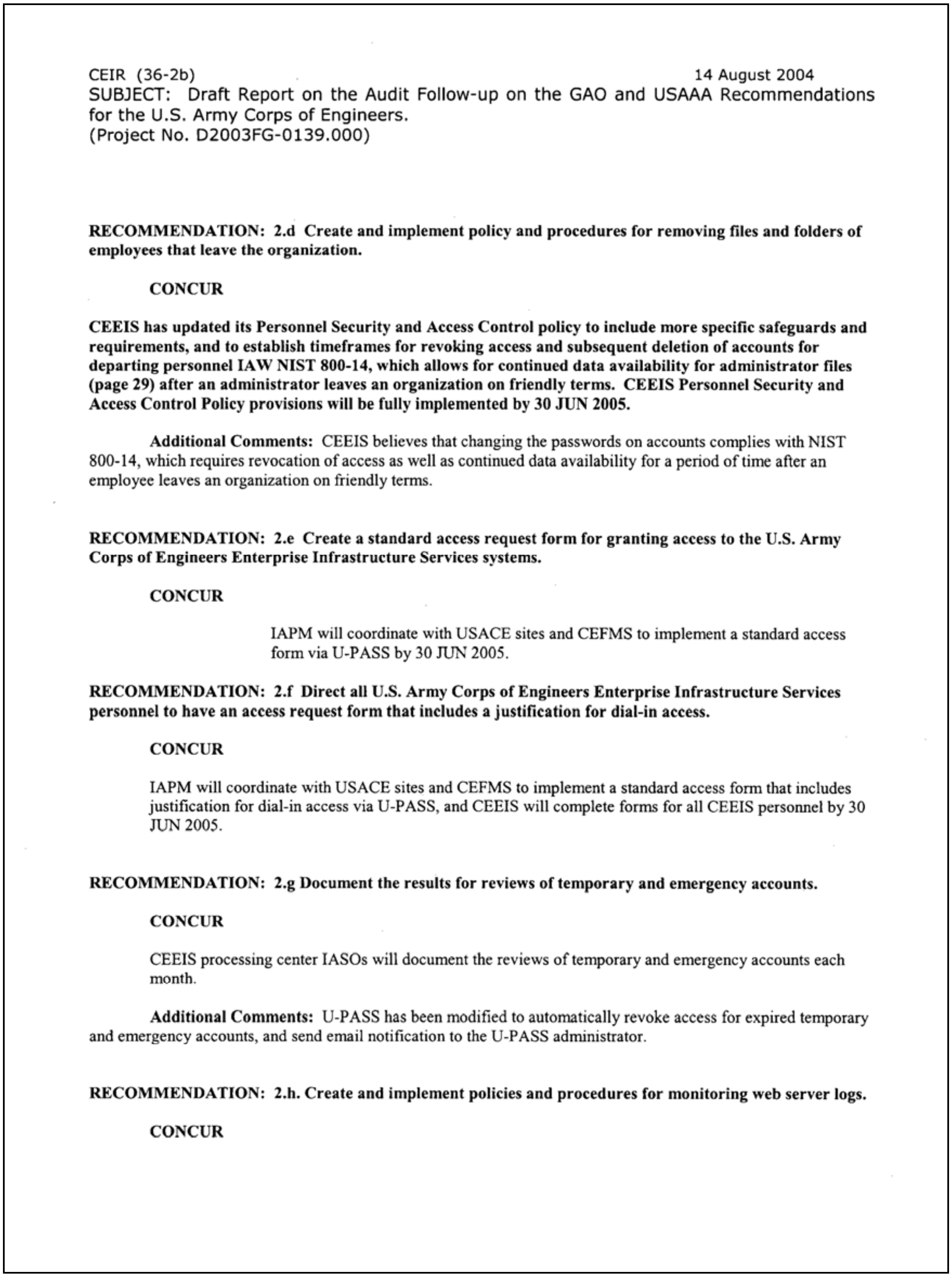
Additional Comments: The USACE shares computing facilities with other DoD organizations to reduce operating and administrative costs associated with its two processing centers, and to support the President's Management Agenda Initiative in the area of Budget and Performance Integration. Physical access is restricted to personnel necessary for CEEIS and the other DoD organizations, as well as facilities, maintenance and cleaning personnel. [CEEIS does not consider personnel authorized by the other DoD organizations as "unauthorized"]; CEEIS personnel are present 24X365 for monitoring the facility with video surveillance of areas outside the line of sight.

RECOMMENDATION: 2.c. Maintain a comprehensive list of personnel that leave U.S. Army Corps of Engineers Enterprise Infrastructure Services.

CONCUR

CEEIS Processing Center IASOs will maintain a list of personnel that separate from employment with CEEIS. Files will be updated by 31 DEC 2004.

Additional Comments: CEEIS will include updating personnel lists as part of center quarterly reviews of the computer room access list.



CEIR (36-2b) 14 August 2004

SUBJECT: Draft Report on the Audit Follow-up on the GAO and USAAA Recommendations for the U.S. Army Corps of Engineers.
(Project No. D2003FG-0139.000)

RECOMMENDATION: 2.d Create and implement policy and procedures for removing files and folders of employees that leave the organization.

CONCUR

CEEIS has updated its Personnel Security and Access Control policy to include more specific safeguards and requirements, and to establish timeframes for revoking access and subsequent deletion of accounts for departing personnel IAW NIST 800-14, which allows for continued data availability for administrator files (page 29) after an administrator leaves an organization on friendly terms. CEEIS Personnel Security and Access Control Policy provisions will be fully implemented by 30 JUN 2005.

Additional Comments: CEEIS believes that changing the passwords on accounts complies with NIST 800-14, which requires revocation of access as well as continued data availability for a period of time after an employee leaves an organization on friendly terms.

RECOMMENDATION: 2.e Create a standard access request form for granting access to the U.S. Army Corps of Engineers Enterprise Infrastructure Services systems.

CONCUR

IAPM will coordinate with USACE sites and CEFMS to implement a standard access form via U-PASS by 30 JUN 2005.

RECOMMENDATION: 2.f Direct all U.S. Army Corps of Engineers Enterprise Infrastructure Services personnel to have an access request form that includes a justification for dial-in access.

CONCUR

IAPM will coordinate with USACE sites and CEFMS to implement a standard access form that includes justification for dial-in access via U-PASS, and CEEIS will complete forms for all CEEIS personnel by 30 JUN 2005.

RECOMMENDATION: 2.g Document the results for reviews of temporary and emergency accounts.

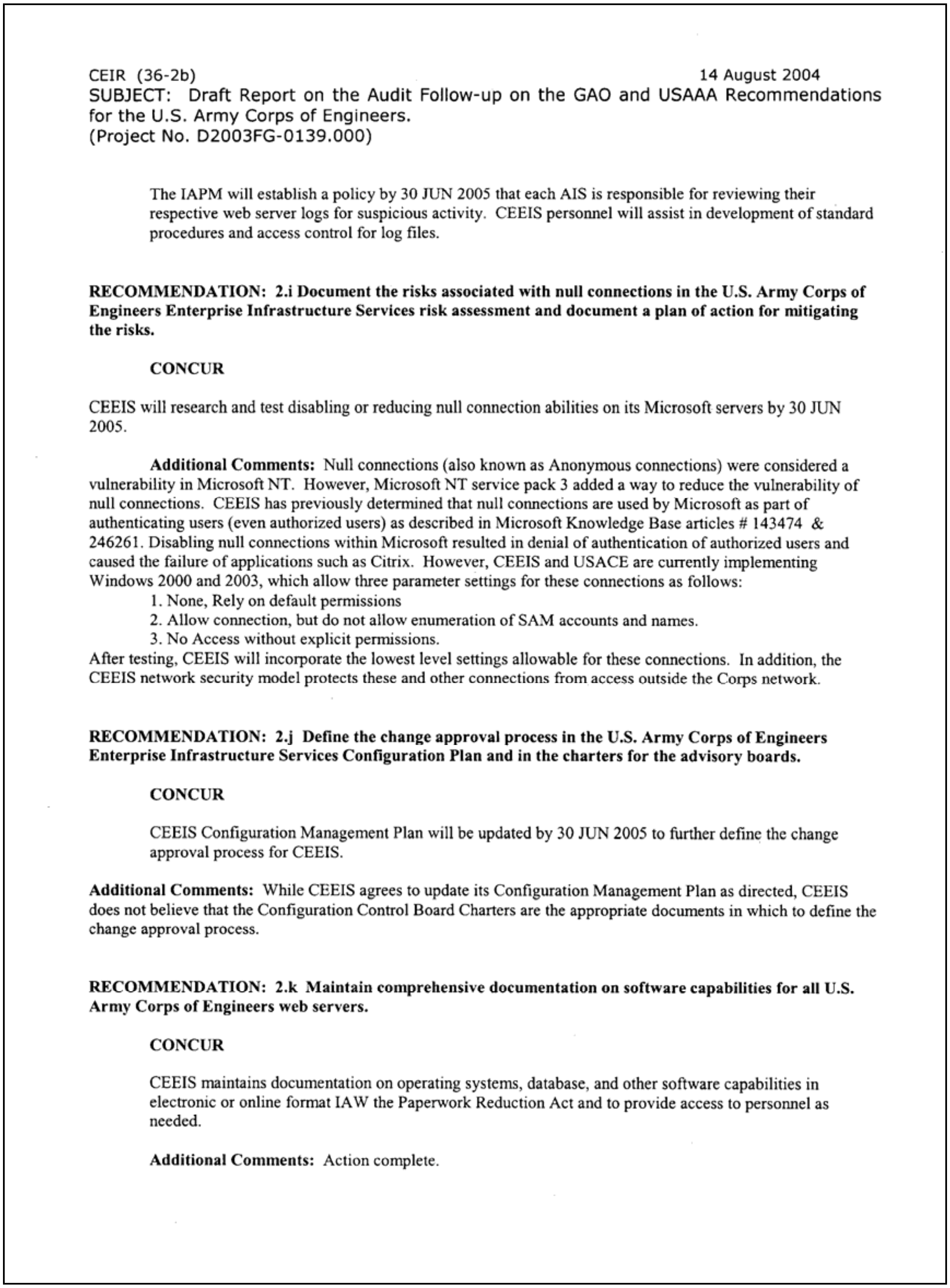
CONCUR

CEEIS processing center IASOs will document the reviews of temporary and emergency accounts each month.

Additional Comments: U-PASS has been modified to automatically revoke access for expired temporary and emergency accounts, and send email notification to the U-PASS administrator.

RECOMMENDATION: 2.h. Create and implement policies and procedures for monitoring web server logs.

CONCUR



CEIR (36-2b) 14 August 2004
SUBJECT: Draft Report on the Audit Follow-up on the GAO and USAAA Recommendations for the U.S. Army Corps of Engineers.
(Project No. D2003FG-0139.000)

The IAPM will establish a policy by 30 JUN 2005 that each AIS is responsible for reviewing their respective web server logs for suspicious activity. CEEIS personnel will assist in development of standard procedures and access control for log files.

RECOMMENDATION: 2.i Document the risks associated with null connections in the U.S. Army Corps of Engineers Enterprise Infrastructure Services risk assessment and document a plan of action for mitigating the risks.

CONCUR

CEEIS will research and test disabling or reducing null connection abilities on its Microsoft servers by 30 JUN 2005.

Additional Comments: Null connections (also known as Anonymous connections) were considered a vulnerability in Microsoft NT. However, Microsoft NT service pack 3 added a way to reduce the vulnerability of null connections. CEEIS has previously determined that null connections are used by Microsoft as part of authenticating users (even authorized users) as described in Microsoft Knowledge Base articles # 143474 & 246261. Disabling null connections within Microsoft resulted in denial of authentication of authorized users and caused the failure of applications such as Citrix. However, CEEIS and USACE are currently implementing Windows 2000 and 2003, which allow three parameter settings for these connections as follows:

1. None, Rely on default permissions
2. Allow connection, but do not allow enumeration of SAM accounts and names.
3. No Access without explicit permissions.

After testing, CEEIS will incorporate the lowest level settings allowable for these connections. In addition, the CEEIS network security model protects these and other connections from access outside the Corps network.

RECOMMENDATION: 2.j Define the change approval process in the U.S. Army Corps of Engineers Enterprise Infrastructure Services Configuration Plan and in the charters for the advisory boards.

CONCUR

CEEIS Configuration Management Plan will be updated by 30 JUN 2005 to further define the change approval process for CEEIS.

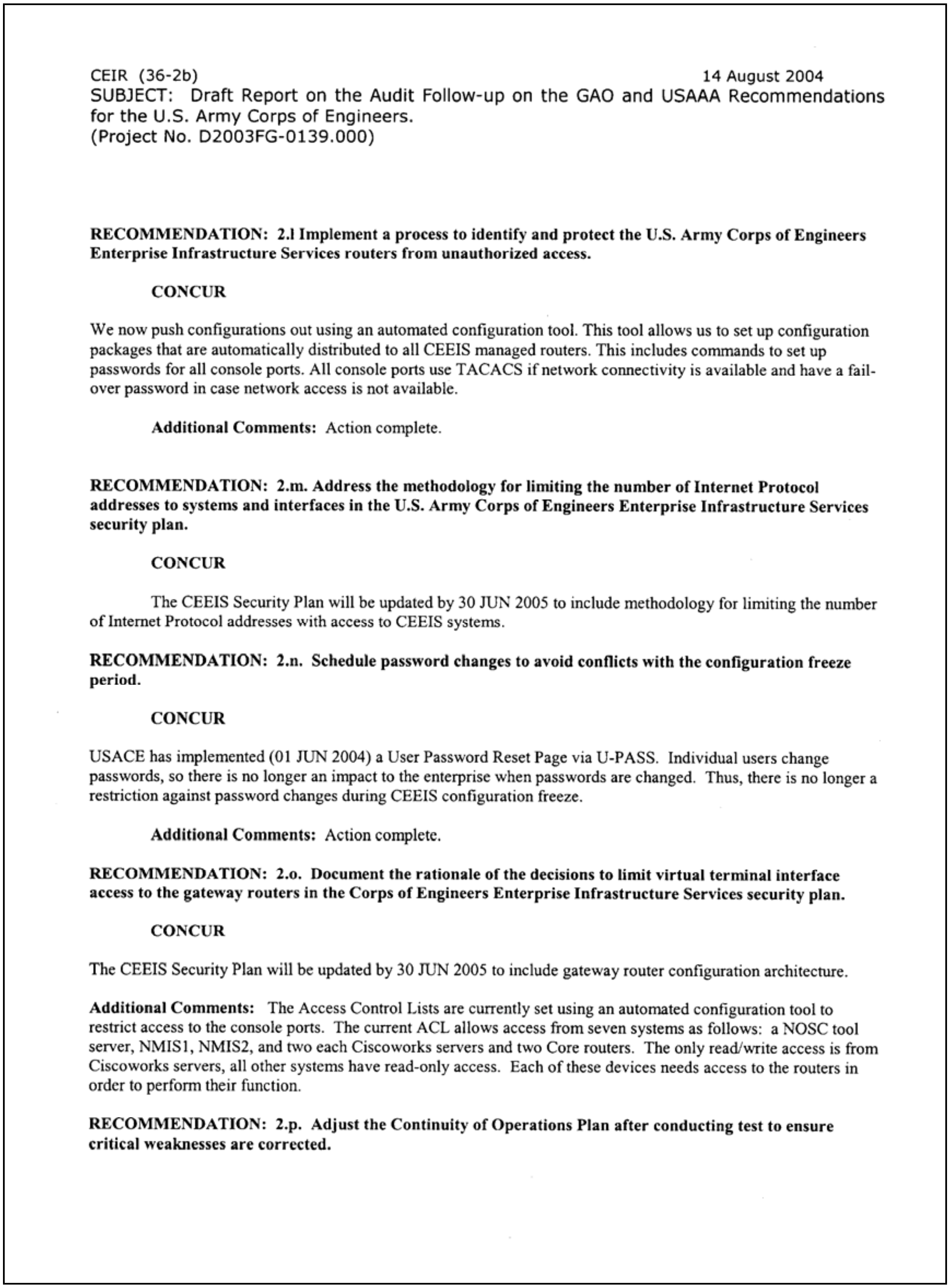
Additional Comments: While CEEIS agrees to update its Configuration Management Plan as directed, CEEIS does not believe that the Configuration Control Board Charters are the appropriate documents in which to define the change approval process.

RECOMMENDATION: 2.k Maintain comprehensive documentation on software capabilities for all U.S. Army Corps of Engineers web servers.

CONCUR

CEEIS maintains documentation on operating systems, database, and other software capabilities in electronic or online format IAW the Paperwork Reduction Act and to provide access to personnel as needed.

Additional Comments: Action complete.



CEIR (36-2b) 14 August 2004
SUBJECT: Draft Report on the Audit Follow-up on the GAO and USAAA Recommendations for the U.S. Army Corps of Engineers.
(Project No. D2003FG-0139.000)

RECOMMENDATION: 2.l Implement a process to identify and protect the U.S. Army Corps of Engineers Enterprise Infrastructure Services routers from unauthorized access.

CONCUR

We now push configurations out using an automated configuration tool. This tool allows us to set up configuration packages that are automatically distributed to all CEEIS managed routers. This includes commands to set up passwords for all console ports. All console ports use TACACS if network connectivity is available and have a fail-over password in case network access is not available.

Additional Comments: Action complete.

RECOMMENDATION: 2.m. Address the methodology for limiting the number of Internet Protocol addresses to systems and interfaces in the U.S. Army Corps of Engineers Enterprise Infrastructure Services security plan.

CONCUR

The CEEIS Security Plan will be updated by 30 JUN 2005 to include methodology for limiting the number of Internet Protocol addresses with access to CEEIS systems.

RECOMMENDATION: 2.n. Schedule password changes to avoid conflicts with the configuration freeze period.

CONCUR

USACE has implemented (01 JUN 2004) a User Password Reset Page via U-PASS. Individual users change passwords, so there is no longer an impact to the enterprise when passwords are changed. Thus, there is no longer a restriction against password changes during CEEIS configuration freeze.

Additional Comments: Action complete.

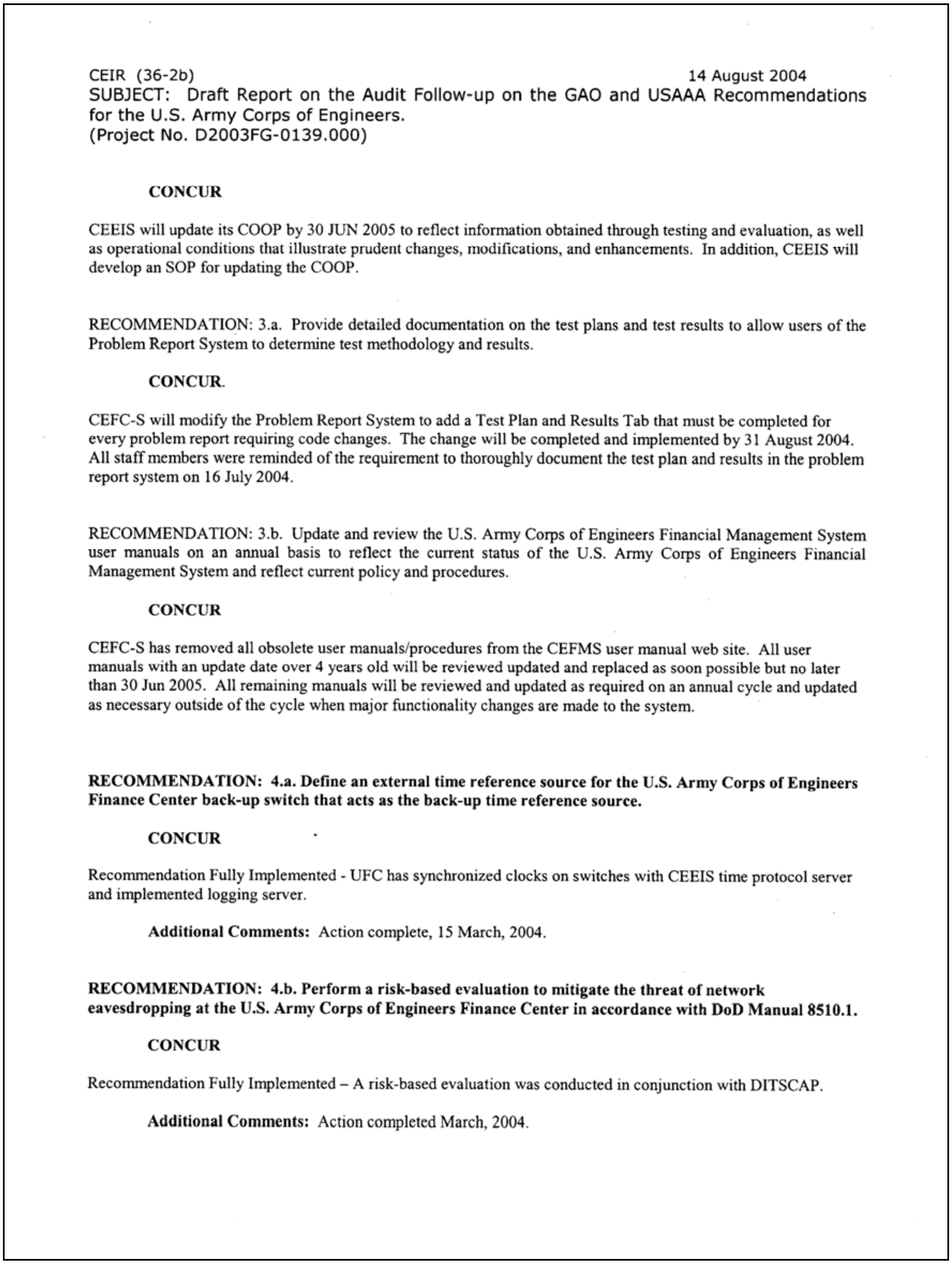
RECOMMENDATION: 2.o. Document the rationale of the decisions to limit virtual terminal interface access to the gateway routers in the Corps of Engineers Enterprise Infrastructure Services security plan.

CONCUR

The CEEIS Security Plan will be updated by 30 JUN 2005 to include gateway router configuration architecture.

Additional Comments: The Access Control Lists are currently set using an automated configuration tool to restrict access to the console ports. The current ACL allows access from seven systems as follows: a NOSC tool server, NMIS1, NMIS2, and two each Ciscoworks servers and two Core routers. The only read/write access is from Ciscoworks servers, all other systems have read-only access. Each of these devices needs access to the routers in order to perform their function.

RECOMMENDATION: 2.p. Adjust the Continuity of Operations Plan after conducting test to ensure critical weaknesses are corrected.



CEIR (36-2b) 14 August 2004

SUBJECT: Draft Report on the Audit Follow-up on the GAO and USAAA Recommendations for the U.S. Army Corps of Engineers.
(Project No. D2003FG-0139.000)

CONCUR

CEEIS will update its COOP by 30 JUN 2005 to reflect information obtained through testing and evaluation, as well as operational conditions that illustrate prudent changes, modifications, and enhancements. In addition, CEEIS will develop an SOP for updating the COOP.

RECOMMENDATION: 3.a. Provide detailed documentation on the test plans and test results to allow users of the Problem Report System to determine test methodology and results.

CONCUR.

CEFC-S will modify the Problem Report System to add a Test Plan and Results Tab that must be completed for every problem report requiring code changes. The change will be completed and implemented by 31 August 2004. All staff members were reminded of the requirement to thoroughly document the test plan and results in the problem report system on 16 July 2004.

RECOMMENDATION: 3.b. Update and review the U.S. Army Corps of Engineers Financial Management System user manuals on an annual basis to reflect the current status of the U.S. Army Corps of Engineers Financial Management System and reflect current policy and procedures.

CONCUR

CEFC-S has removed all obsolete user manuals/procedures from the CEFMS user manual web site. All user manuals with an update date over 4 years old will be reviewed updated and replaced as soon possible but no later than 30 Jun 2005. All remaining manuals will be reviewed and updated as required on an annual cycle and updated as necessary outside of the cycle when major functionality changes are made to the system.

RECOMMENDATION: 4.a. Define an external time reference source for the U.S. Army Corps of Engineers Finance Center back-up switch that acts as the back-up time reference source.

CONCUR

Recommendation Fully Implemented - UFC has synchronized clocks on switches with CEEIS time protocol server and implemented logging server.

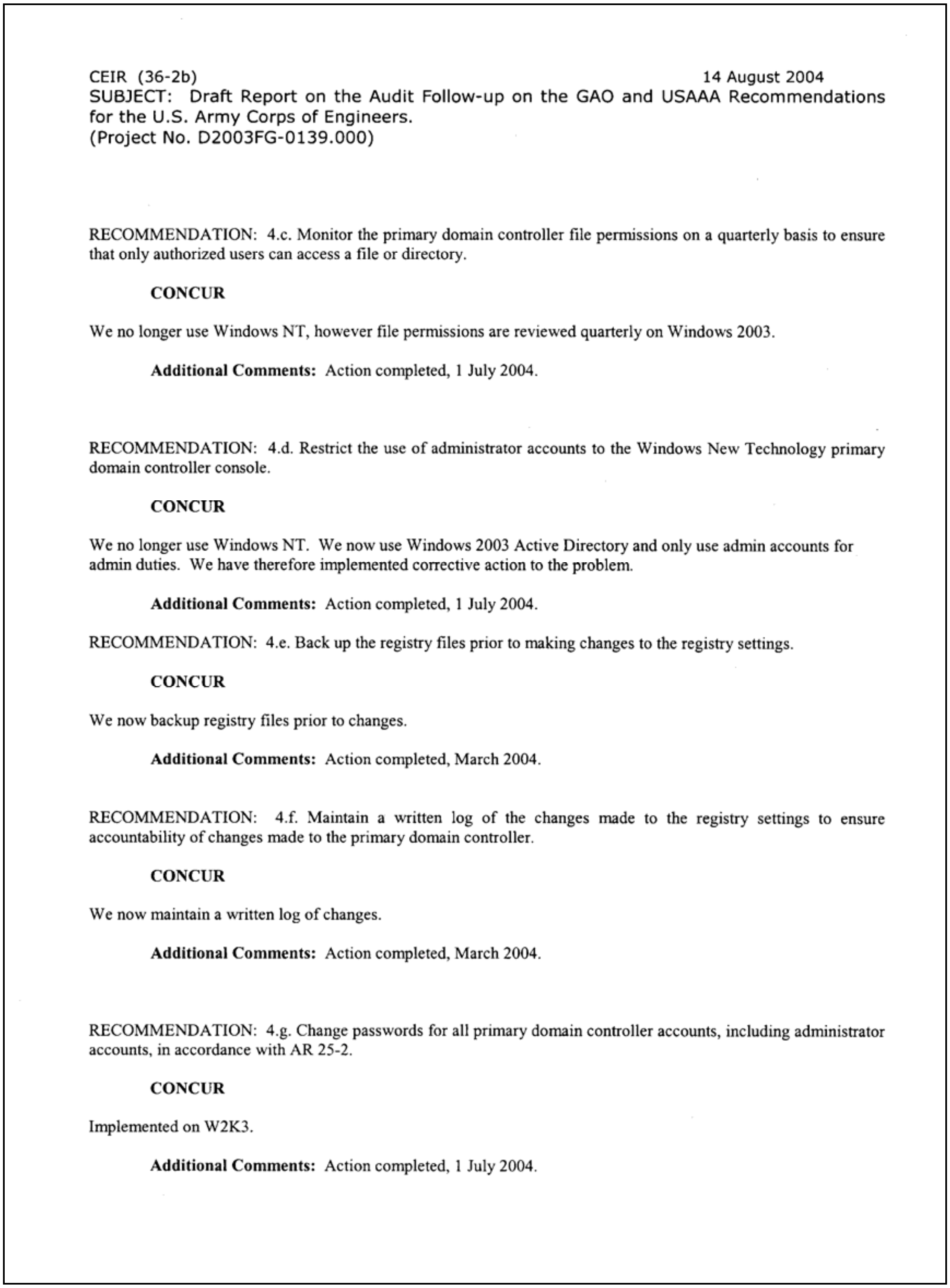
Additional Comments: Action complete, 15 March, 2004.

RECOMMENDATION: 4.b. Perform a risk-based evaluation to mitigate the threat of network eavesdropping at the U.S. Army Corps of Engineers Finance Center in accordance with DoD Manual 8510.1.

CONCUR

Recommendation Fully Implemented – A risk-based evaluation was conducted in conjunction with DITSCAP.

Additional Comments: Action completed March, 2004.



CEIR (36-2b) 14 August 2004

SUBJECT: Draft Report on the Audit Follow-up on the GAO and USAAA Recommendations for the U.S. Army Corps of Engineers.
(Project No. D2003FG-0139.000)

RECOMMENDATION: 4.c. Monitor the primary domain controller file permissions on a quarterly basis to ensure that only authorized users can access a file or directory.

CONCUR

We no longer use Windows NT, however file permissions are reviewed quarterly on Windows 2003.

Additional Comments: Action completed, 1 July 2004.

RECOMMENDATION: 4.d. Restrict the use of administrator accounts to the Windows New Technology primary domain controller console.

CONCUR

We no longer use Windows NT. We now use Windows 2003 Active Directory and only use admin accounts for admin duties. We have therefore implemented corrective action to the problem.

Additional Comments: Action completed, 1 July 2004.

RECOMMENDATION: 4.e. Back up the registry files prior to making changes to the registry settings.

CONCUR

We now backup registry files prior to changes.

Additional Comments: Action completed, March 2004.

RECOMMENDATION: 4.f. Maintain a written log of the changes made to the registry settings to ensure accountability of changes made to the primary domain controller.

CONCUR

We now maintain a written log of changes.

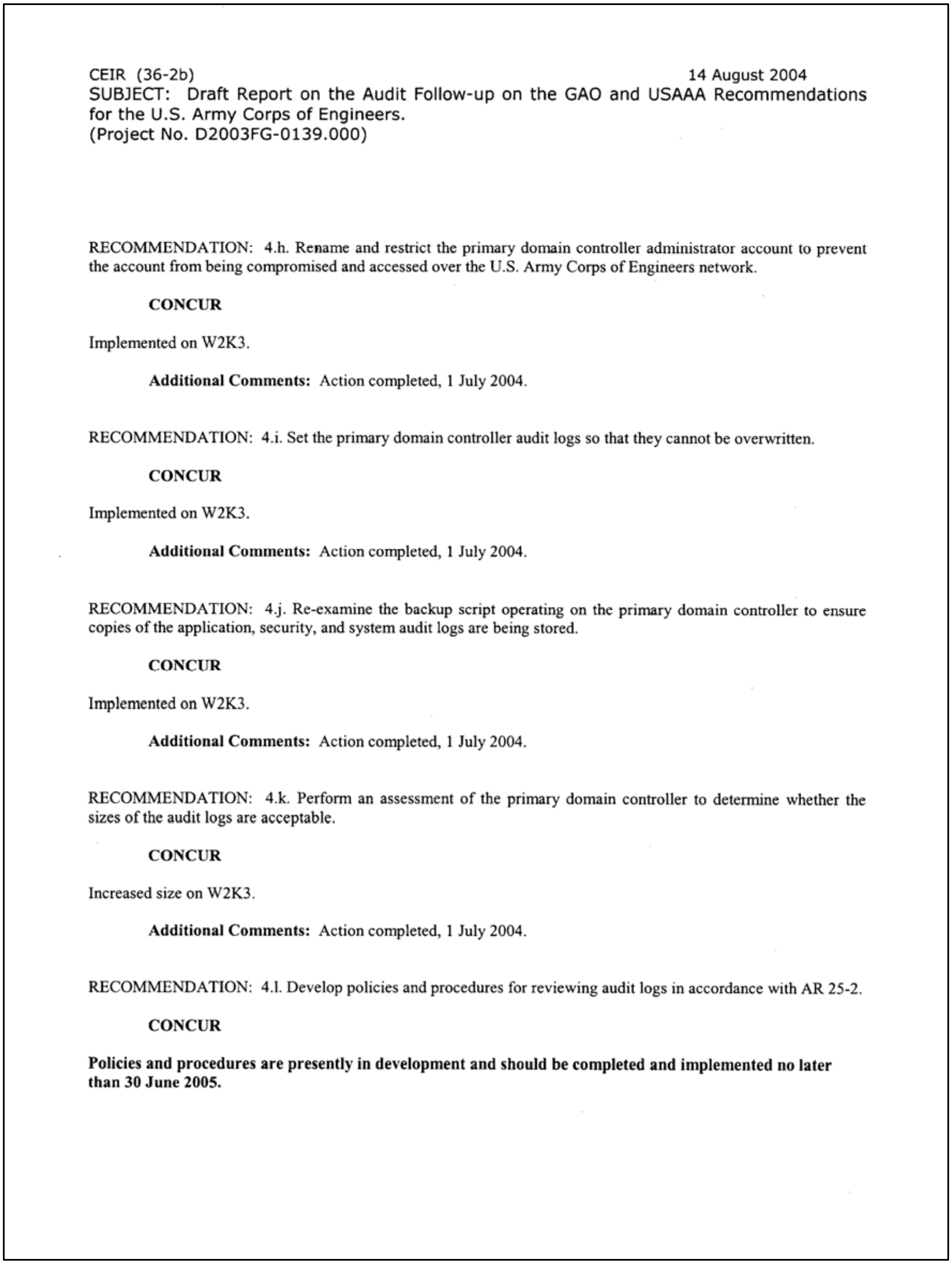
Additional Comments: Action completed, March 2004.

RECOMMENDATION: 4.g. Change passwords for all primary domain controller accounts, including administrator accounts, in accordance with AR 25-2.

CONCUR

Implemented on W2K3.

Additional Comments: Action completed, 1 July 2004.



CEIR (36-2b) 14 August 2004
SUBJECT: Draft Report on the Audit Follow-up on the GAO and USAAA Recommendations for the U.S. Army Corps of Engineers.
(Project No. D2003FG-0139.000)

RECOMMENDATION: 4.h. Rename and restrict the primary domain controller administrator account to prevent the account from being compromised and accessed over the U.S. Army Corps of Engineers network.

CONCUR

Implemented on W2K3.

Additional Comments: Action completed, 1 July 2004.

RECOMMENDATION: 4.i. Set the primary domain controller audit logs so that they cannot be overwritten.

CONCUR

Implemented on W2K3.

Additional Comments: Action completed, 1 July 2004.

RECOMMENDATION: 4.j. Re-examine the backup script operating on the primary domain controller to ensure copies of the application, security, and system audit logs are being stored.

CONCUR

Implemented on W2K3.

Additional Comments: Action completed, 1 July 2004.

RECOMMENDATION: 4.k. Perform an assessment of the primary domain controller to determine whether the sizes of the audit logs are acceptable.

CONCUR

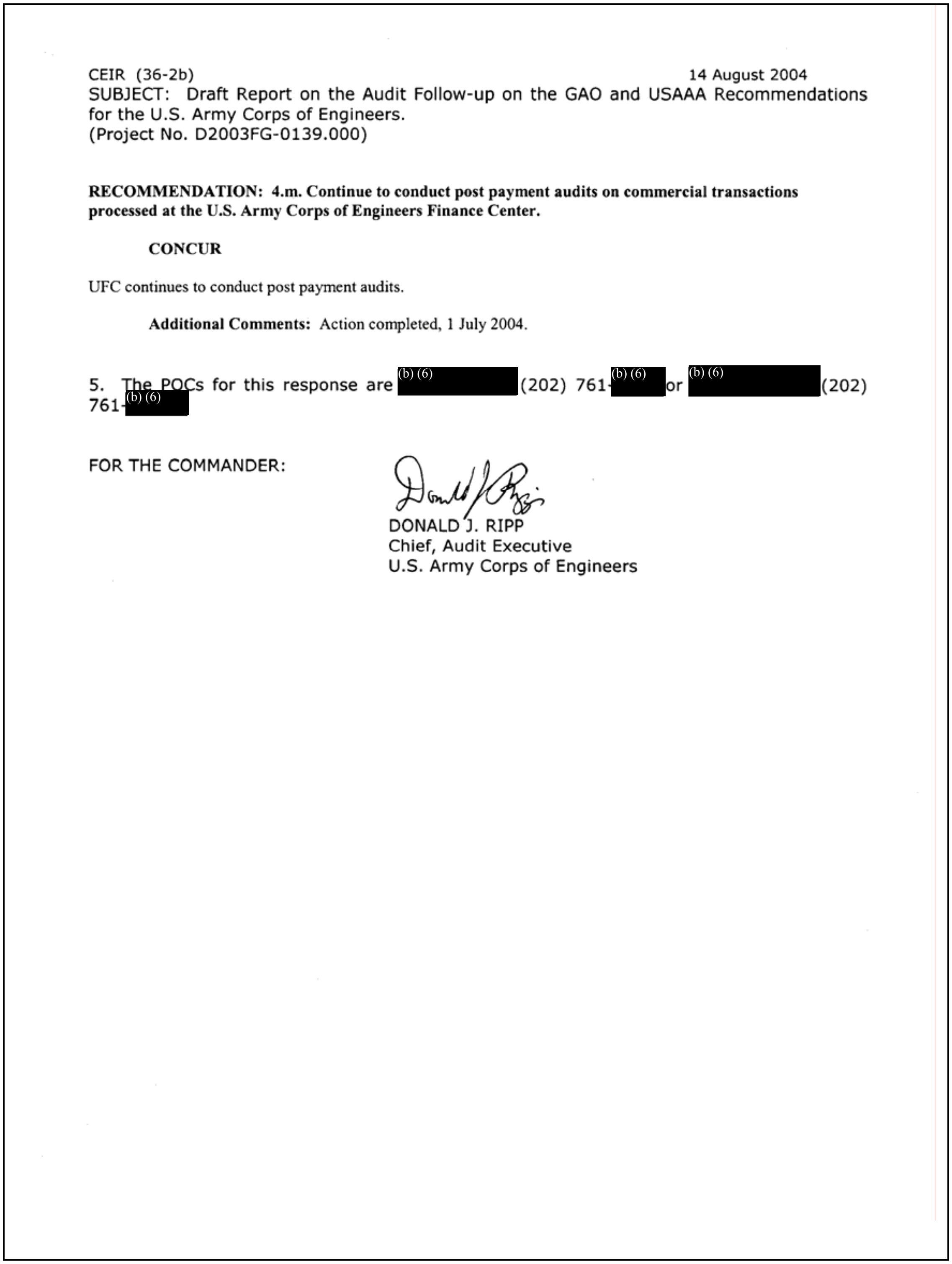
Increased size on W2K3.

Additional Comments: Action completed, 1 July 2004.

RECOMMENDATION: 4.l. Develop policies and procedures for reviewing audit logs in accordance with AR 25-2.

CONCUR

Policies and procedures are presently in development and should be completed and implemented no later than 30 June 2005.



CEIR (36-2b) 14 August 2004

SUBJECT: Draft Report on the Audit Follow-up on the GAO and USAAA Recommendations for the U.S. Army Corps of Engineers.
(Project No. D2003FG-0139.000)

RECOMMENDATION: 4.m. Continue to conduct post payment audits on commercial transactions processed at the U.S. Army Corps of Engineers Finance Center.

CONCUR

UFC continues to conduct post payment audits.

Additional Comments: Action completed, 1 July 2004.

5. The POCs for this response are (b) (6) (202) 761-(b) (6) or (b) (6) (202) 761-(b) (6)

FOR THE COMMANDER:

DONALD J. RIPP
Chief, Audit Executive
U.S. Army Corps of Engineers

Team Members

The Office of the Deputy Inspector General for Auditing of the Department of Defense, Defense Financial Auditing Service prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

(b) (6)

[redacted]

U.S. Army 1st Information Operations Command

(b) (6)

[redacted]