United States General Accounting Office

GAO

Report to the Commanding General,
U.S. Army Corps of Engineers

June 2002

INFORMATION SECURITY

Corps of Engineers Making Improvements, But Weaknesses Continue

GAO-02-589

G A O
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

June 10, 2002

Lt. General Robert B. Flowers, USA
Commanding
U.S. Army Corps of Engineers

Dear General Flowers:

In connection with our requirement to audit the annual U.S. government consolidated financial statements[1] and in support of the Army Audit Agency's audit of the financial statements of the U.S. Army Corps of Engineers, Civil Works, we tested selected general and application controls[2] over the Corps of Engineers Financial Management System (CEFMS). The U.S. Army Corps of Engineers relies on CEFMS to perform key financial management functions supporting the Corps' military and civil works missions.

We previously reported (for fiscal year 1999) on general and application control weaknesses that placed CEFMS at significant risk of unauthorized disclosure and modification of sensitive data and programs, misuse or damage to computer resources, or disruption of critical operations.[3]

For the current engagement, our objective was to evaluate the design and test the effectiveness of selected Corps general and application computer controls over CEFMS for fiscal year 2001. In doing so, we also assessed the corrective actions taken by the Corps to address the weaknesses that we

[1]31 U.S.C. 331(e) (1994).

[2]Information system general controls affect the overall effectiveness and security of computer operations, as opposed to being unique to any specific computer application. They include security management, operating procedures, software security features, and physical protection designed to ensure that access to data is appropriately restricted, only authorized changes are made to computer programs, computer security duties are segregated, and backup and recovery plans are adequate to ensure the continuity of essential operations. Application controls relate directly to the individual computer programs that are used to perform transactions. They help to further ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.

[3]U.S. General Accounting Office, *Financial Management: Significant Weaknesses in Corps of Engineers' Computer Controls*, GAO-01-89 (Washington, D.C.: October 11, 2000).

identified during our fiscal year 1999 review.[4] This report also includes a summary (based on work led by the Army Audit Agency) of general control weaknesses associated with Corps entitywide security management and service continuity.

Separately, we issued a "Limited Official Use Only" report to you detailing the results of our review. This version of the report, for public release, provides a general summary of the vulnerabilities identified and our recommendations to help strengthen and improve CEFMS general and application controls. (The "Limited Official Use Only" report provided technical details to assist the Corps in implementing the recommendations that we made.)

Results in Brief

The Corps has made substantial progress in improving computer controls at each of its data processing centers and other Corps sites since our 1999 review. Of the 93 recommendations that we made, the Corps had completed action on 54 and partially completed or had action plans to correct the remaining 39. During our current review, the Corps also corrected 9 newly identified weaknesses.

Nevertheless, continuing and newly identified vulnerabilities involving general and application computer controls continue to impair the Corps' ability to ensure the reliability, confidentiality, and availability of financial and sensitive data. These vulnerabilities warrant management's attention to decrease the risk of inappropriate disclosure and modification of data and programs, misuse of or damage to computer resources, or disruption of critical operations. Such vulnerabilities also increase risks to other Department of Defense (DOD) networks and systems to which the Corps' network is linked.

Weaknesses in general controls impaired the Corps' ability to ensure, for example, that (1) computer risks are adequately assessed, and security policies and procedures within the organization are effective and consistent with overall organizational policies and procedures; (2) users have only the access needed to perform their duties; (3) system software changes are properly documented before being placed in operation; (4) test

[4]Fiscal year 1999 review refers to work performed in support of Army Audit Agency's audit of the Corps of Engineers, Civil Works, fiscal year 1999 financial statements. The audit work was performed from September 1999 through January 2000.

plans and results for application changes are formally documented; (5) duties and responsibilities are adequately segregated; (6) critical applications are properly restored in the case of a disaster or interruption; and (7) the Corps has adequately protected its network from unauthorized traffic.

Application control weaknesses impaired the Corps' ability to ensure that (1) current and accurate CEFMS access authorizations are maintained, (2) user manuals reflect the current CEFMS environment, and (3) the Corps is effectively using electronic signature capabilities. Further, tests by the Army Audit Agency have identified instances where CEFMS electronic signature smartcards[5] were not under the sole control of an individual smartcard holder. As a result, authentication controls were not effective to provide reasonable assurance that users' electronic signatures are valid.

To assist Corps management in addressing these computer control weaknesses (summarized in this report), we have made recommendations that will help strengthen and improve CEFMS general and application controls. In providing written comments on this report, the commanding general of the U.S. Army Corps of Engineers concurred with our recommendations and noted their plans to correct the information security weaknesses.

Background

The U.S. Army Corps of Engineers, made up of approximately 34,600 civilian and 650 military personnel, has both military and civil works missions. The Corps' military mission includes managing and executing engineering, construction, and real estate programs for DOD components, other federal agencies, state and local governments, and foreign governments. The Corps also provides military support by managing and executing Army installation support programs and by developing and maintaining the capability to mobilize in response to national security emergencies. The Corps' civil works program involves investigating, developing, and maintaining the nation's water and related environmental resources; constructing and operating projects for navigation; developing hydroelectric power; and conserving fish and wildlife.

[5]Smartcards, which are similar in size and shape to credit cards, are issued to each authorized central security officer, district security officer, systems administrator, and user so that they can gain access to the electronic signature system. The smartcard contains a microprocessor chip that stores data needed for signature generation.

The Corps is organized geographically into eight divisions in the United States and 41 subordinate districts throughout the United States, Asia, and Europe.[6] The districts oversee project offices throughout the world. The Corps also has eight research laboratories and two data processing centers. Further, the Corps conducts business with numerous external customers, including the military departments and various federal government agencies. External customers require access to the Corps' systems for such things as posting and retrieval of information for water management functions.

The Corps' Finance Center has centralized responsibility for issuing checks and electronic funds transfers for the various Corps sites and external customers. During fiscal year 2000, CEFMS made about $11 billion in disbursements for Corps (civil works and military fund) activities.

The Corps acquired and owns the Corps of Engineers Enterprise Information System (CEEIS) wide area network, which supports multiple unclassified Corps systems, including its key financial management system, CEFMS. The CEEIS interconnects Corps sites worldwide, providing for the exchange of traffic between sites in support of engineering, financial management, E-mail, and real-time data collection. External customers access Corps systems via the Internet and DOD's Unclassified (but Sensitive) Internet Protocol Router Network (NIPRNet) gateways at selected sites. CEFMS processes financial and other data at two data processing centers. Each Corps site maintains its own database and provides its financial data input to one of the two processing centers. Corps users enter data and update financial transactions in CEFMS via workstations at the various organizational elements.

Objective, Scope, and Methodology

Our objective was to evaluate the design and test the effectiveness of selected general and application controls over CEFMS. Our work included assessing (1) the corrective actions taken by the Corps to address the weaknesses that we identified during our fiscal year 1999 general and application control review of CEFMS; and (2) the effectiveness of the Corps' computer controls to help ensure the reliability, availability, and confidentiality of financial and sensitive data contained in CEFMS.

[6]Of the 41 districts, 38 have both military and civil works missions. The remaining 3 districts (Korea, Japan, and Europe) have only a military mission.

We contracted with an independent public accounting firm, PricewaterhouseCoopers (PwC), LLP, to assist in the evaluation and testing of CEFMS computer controls. We determined the scope of our contractor's audit work, monitored its progress, attended key meetings between PwC and Corps personnel, and reviewed the related working papers. PwC used our *Federal Information System Controls Audit Manual*[7] (FISCAM) to guide the general controls testing. This testing included four of the six FISCAM general control areas: (1) access controls, (2) application software development and change control, (3) systems software, and (4) segregation of duties. PwC used a proprietary methodology tailored to CEFMS to evaluate and test application controls over selected CEFMS modules.

The Army Audit Agency evaluated the two remaining FISCAM areas: entitywide security management and service continuity. Working with the Army Audit Agency for these two FISCAM areas, we analyzed DOD, Department of the Army, and Corps information assurance documents; interviewed key personnel to document responsibilities, actions, and plans for Corps-wide information security management, information technology, and operations management; and evaluated Corps security program elements against GAO, DOD, Army, and other federal criteria. The Army Audit Agency plans to issue a report on these two FISCAM areas in fiscal year 2002.

Our fiscal year 2001 review also included a network vulnerability assessment of a critical path between two Corps network segments.

During the course of our work, we communicated our findings to Corps officials, who informed us of the corrective actions they planned or had taken to address many of the weaknesses we identified.

Our review was performed from January to October 2001 at the two Corps data processing centers; the Corps Finance Center; the CEFMS Development Center; and 3 of the 41 Corps districts. These districts were chosen because of the significance of their processing volumes. We also held interviews with Corps officials at the Corps Headquarters in Washington, D.C. Our work was performed in accordance with generally accepted government auditing standards.

[7]U.S. General Accounting Office, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

General Control Weaknesses Place CEFMS at Risk

General controls—the structures, policies, and procedures that apply to an entity's overall computer operations—establish the environment in which application systems and controls operate. An effective general controls environment would (1) ensure that an adequate computer security management program is in place; (2) protect data, files, and programs from unauthorized access, modification, and destruction; (3) limit and monitor access to programs and files that protect applications and control computer hardware; (4) prevent unauthorized changes to systems and applications software; (5) prevent any one individual from controlling key aspects of computer-related operations; (6) ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption; and (7) ensure that only authorized individuals can gain network access to sensitive and critical agency data.

Of the 75 recommendations that we made on general controls in our fiscal year 1999 audit, the Corps had completed action on 41 and had partially completed or was implementing action plans to correct the remaining 34. Among the actions taken, the Corps had (for example)

- reconfigured its network, including implementing firewalls and deploying intrusion detection systems;
- deleted certain unneeded/vulnerable services operating on CEFMS servers;
- performed auditing on changes made to the CEFMS access control table;
- enforced monitoring of system log files on the CEFMS servers;
- formalized Corps policies and procedures for making and documenting CEFMS changes and for obtaining approvals on user acceptance tests resulting from software changes; and
- updated job descriptions at data centers to better address the concept of segregation of duties.

Although the Corps made substantial progress in correcting vulnerabilities, continuing and newly identified vulnerabilities in general computer controls continue to impair the Corps' ability to ensure the reliability, confidentiality, and availability of financial and sensitive data. In addition

to the results of our review, Corps records indicate that from October 2000 through June 2001 vulnerabilities in Corps systems resulted in several serious compromises.

The numbers in table 1 reflect open recommendations on general controls, including both recommendations remaining from our fiscal year 1999 review and additional recommendations arising from our fiscal year 2001 review.

Table 1: Recommendations by General Control Area

Area of control	FY 1999 outstanding recommendations	FY 2001 recommendations[a]
Security management[b]	—[b]	—[b]
Access controls	26	22
System software	5	5
Application software development & change control	1	3
Segregation of duties	2	4
Service continuity[b]	—[b]	—[b]
Network security	—[c]	21
Total	**34**	**55**

[a] Among these fiscal year 2001 recommendations are seven that address weaknesses corrected during our fieldwork.

[b] The Army Audit Agency performed the audit of these areas and plans to report its recommendations separately. This report summarizes weaknesses identified in these areas.

[c] Network security was not separately identified in the fiscal year 1999 review.

Corps' Entitywide Security Management Program Is Not Yet Effective

The foundation of an entity's security control structure is an entitywide program for security management, which should establish a framework for continually (1) assessing risk, (2) developing and implementing effective security procedures, and (3) monitoring and evaluating the effectiveness of security procedures. A well-designed entitywide security management program helps to ensure that security controls are adequate, properly implemented, and applied consistently across the entity and that responsibilities are clearly understood. In our May 1998 best practices guide on information security management at leading nonfederal

organizations,[8] we reported that leading organizations successfully managed their information security risks through an ongoing cycle of risk management activities.

As we discussed in our fiscal year 1999 report, an underlying cause for the Corps' computer control weaknesses was that it did not yet have an effective security management program. The lack of an effective security management program increases the risk that computer control weaknesses could exist and not be detected promptly so that losses or disruptions could be prevented. For fiscal year 1999, the Army Audit Agency identified four weaknesses in the Corps' security management program and issued five recommendations to address the weaknesses.[9] The Army Audit Agency reported that key elements of an entitywide security program were needed, including a more comprehensive program definition in an entitywide security plan, updated network accreditation and risk assessments, and complete and documented background investigations. Also, the Army Audit Agency reported that other key elements were immature, including assignment of security responsibilities, a formal incident response team, computer security training, and security policy assessment and compliance verification.

Since our fiscal year 1999 audit, the Corps has taken several steps to define and develop an agencywide security program. It has established a central focal point for information assurance at Corps Headquarters, consisting of an information assurance program manager and staff reporting to the Architecture Branch of Information Technology Services under the chief information officer. The staff includes a coordinator for Corps security accreditation activities. A 5-year budget has been developed for Corps-wide investments in information security technologies and services, and several agencywide information assurance initiatives are planned, including public key infrastructure, risk assessment, and automated system vulnerability updates.

The Corps has appointed information assurance managers and officers throughout its functional units and assigned them responsibility for implementing the Army's security regulations. It has also identified training

[8]U.S. General Accounting Office, *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

[9]Army Audit Agency, *Corps of Engineers Financial Management System: General and Application Controls*, AA 01-319 (June 26, 2001).

requirements for these and other positions. In addition, the Corps has established processes for notification and reporting on DOD's information assurance vulnerability alerts and has begun updating system security accreditations under DOD's Defense Information Technology Security Certification and Accreditation Program. These elements are necessary to meet federal guidance and DOD and Army requirements for protection of automated information systems.

Although the Corps has identified and addressed some near-term security priorities, it has not yet developed a comprehensive management program to ensure that its information security policies and practices are fully defined, consistent, and continuously effective across all systems, facilities, and organizational levels. Specifically,

- the Corps has not yet developed a comprehensive information assurance program plan that ensures appropriate security posture and adequate security resources for all systems, facilities, and programs, and supports agency-level monitoring of progress toward security objectives;

- information security policy, plans, and procedures are incomplete in areas such as risk assessment, cyber incident management, and personnel security, and limited guidance has been provided to functional units for implementing policy and plans;

- current mechanisms for identifying system vulnerabilities and ensuring appropriate corrective actions are limited, and as a result, systems remain vulnerable to inappropriate access, inadequate physical security, and users with incomplete and missing background investigations;

- processes for monitoring and evaluating security measures throughout the Corps (such as command staff inspections, vulnerability assessments, and reviews of the effectiveness of corrective actions taken) have not been sufficiently frequent or rigorous to be fully effective in identifying security policy violations, system vulnerabilities, and weaknesses in operational controls; and

- an agencywide incident response capability has not been fully implemented in areas such as centralized incident tracking, follow-up, and evidence controls.

The Army Audit Agency plans to issue a report in fiscal year 2002 providing additional discussion on these weaknesses.

Access Controls Were Not Adequate

Access controls should be designed to limit or detect unauthorized access to computer programs, data, equipment, and facilities, so that these resources are protected from unauthorized modification, disclosure, loss, or impairment. Such controls include both logical access controls and physical security controls.

Logical access controls involve the protection of data supporting critical operations from unauthorized access. Organizations can protect these data by requiring users to input unique user identifications, passwords, or other identifiers that are linked to predetermined access privileges and by providing a log of security events. Logical access controls prevent unauthorized user access to computing resources and restrict the access of legitimate users to the specific systems, programs, and files they need to conduct their work.

Physical security controls include surveillance personnel and equipment, locks, guards, ID badges, alarms, and similar measures that limit access to the buildings and rooms where computer facilities and resources are housed, thus helping to safeguard them from intentional or unintentional loss or impairment.

A key weakness in Corps' controls was that it had not appropriately limited user access. Although the Corps developed a security audit script to assist database administrators (DBAs) in identifying security practices that are inconsistent with user management principles, we found instances of inappropriate user access and weaknesses in user management, including those described below.

Weak password management. Sensitive CEFMS administrative-level accounts had passwords that could be easily guessed, which could allow unauthorized access to CEFMS data.

Inadequate management of user IDs. CEFMS users were assigned sensitive administrative-level privileges that either could not be justified by the DBAs or were not needed to perform the users' job functions. As a result, the risk is increased that CEFMS data could be compromised without detection.

Inappropriate access privileges. All CEFMS users, regardless of their job functions, had access privileges to certain tables on their local databases that allowed them to make changes to CEFMS data outside the CEFMS application. As a result, the risk is increased that CEFMS users could make inappropriate changes to CEFMS data.

Command line access. CEFMS users continued to have the ability to log in directly to the operating system, giving users the ability to execute many commands that are not necessary to access CEFMS, as well as the opportunity to take advantage of vulnerable programs, files, and directories. Further, since user commands were not audited, there was no method to identify whether users were attempting to issue unauthorized commands.

Inadequate monitoring of audit logs. Audit logs were not used to detect and monitor security violations, thereby increasing the risk that violations could occur undetected.

Informal procedures for access requests. Access request procedures for privileged or dial-in access to the CEFMS servers were not adequately enforced, thereby increasing the risk that employees without a legitimate or authorized need could gain such access.

Weak passwords on Corps dial-in servers. Corps dial-in modems at one site (non-CEFMS) contained easily guessed usernames and passwords. Such access places Corps network assets at risk.

Lack of monitoring of Web server activity. The Corps was not monitoring CEFMS Web server activity or reviewing and analyzing log files, thereby increasing the risk that attempted intrusion or potential degradation of service could go unnoticed.

System Software Controls Were Not Adequate to Protect Programs and Sensitive Files

To protect the overall integrity and reliability of information systems, it is essential to control access to and modifications of system software. System software controls, which limit and monitor access to the powerful programs and sensitive files associated with computer operations, are important in providing reasonable assurance that access controls are not compromised and that the operating system will not be impaired. To protect system software, a standard computer control practice is to (1) configure system software to protect against security vulnerabilities, (2) periodically review sensitive software to identify potential security

weaknesses, and (3) ensure that only authorized and fully tested system software is placed in operation.

While the Corps had corrected many of the system software weaknesses that we identified in our fiscal year 1999 audit, we identified other weaknesses where the Corps was not adequately controlling system software. These weaknesses included the following.

Unencrypted usernames and passwords over the network. Corps usernames and passwords continued to be sent unencrypted over the network. Consequently, an individual with physical access to a site's local network could capture usernames and passwords and then use that information to gain unauthorized access to the database. The attacker might also be able to use this information to gain additional privileges on the local network.

Ineffective authentication controls over Corps servers. Corps servers continued to allow unauthenticated connections, thereby increasing the risk that an attacker could gather information to gain further access to the system or that other DOD networks could be attacked via the Corps' network.

Lack of formal test plans and procedures for validating operating system upgrades. The Corps had no formal test plans and procedures to ensure system integrity after operating system software upgrades were performed, thereby increasing the risk that some processing functions might not operate properly after a system upgrade.

Changes to Application Software Programs Were Not Adequately Controlled

Controls over the design, development, and modification of application software help to ensure that all programs and program modifications are properly authorized, tested, and approved before they are placed in operation and that access to and distribution of programs are carefully controlled. These controls also help prevent security features from being inadvertently or deliberately turned off, audit logs from being modified, and processing irregularities or malicious code from being introduced.

Changes to application software programs were not adequately documented or controlled. Described below are some examples of the application change control weaknesses that we identified.

Lack of documented test plans and results. The Corps did not formally document test plans and test results for CEFMS software changes, increasing the risk that developers might unknowingly introduce processing anomalies or make unauthorized changes.

Informal Web server change management. At one data processing center, a Web server change management program was not documented or formalized, nor did the center have a lead Web administrator to coordinate changes. Also, the other data processing center did not have a current change control program for its Web server. Without a strong change management process, unauthorized changes could be made to the Web server application.

Demonstration files on production Web servers. CEFMS production Web servers contained vendor demonstration files with known vulnerabilities that are easily exploitable, increasing the risk that an attacker could gain unauthorized access to CEFMS.

Information Management Duties Were Not Always Properly Segregated

A key control for safeguarding programs and data is to ensure that staff duties and responsibilities for authorizing, processing, recording, and reviewing data, as well as for initiating, modifying, migrating, and testing programs, are separated to reduce the risk that errors or fraud will occur and go undetected. Incompatible duties that should be segregated include application and system programming, production control, database administration, computer operations, and data security. Once policies and job descriptions supporting the principles of segregation of duties have been developed, it is important to ensure that adequate supervision is provided and adequate access controls are in place to ensure that employees perform only compatible functions.

Although computer duties were generally properly segregated, we identified instances where controls did not enforce segregation of duties principles, as in the following examples.

Lack of reviews and training regarding segregation of duties concepts. We found that training at the data processing centers did not address segregation of duties principles. If employees are not properly trained in segregation of duties principles, managers may find it difficult to hold employees accountable if they perform incompatible duties.

Also, the data processing centers had not performed reviews to determine whether incompatible duties were appropriately segregated. Without periodically reviewing individuals' roles and responsibilities, management cannot be assured that appropriate segregation of duties is being maintained. They may also find it difficult to hold employees accountable for using their access privileges to carry out inappropriate activity.

Development staff given access to production systems. CEFMS developers had inappropriate access to the CEFMS production databases. We identified several instances in which developers had excessive privileges. Allowing application development staff access to the production environment increases the likelihood that unauthorized changes could be made to the production environment.

Service Continuity Planning Was Not Complete

An organization's ability to accomplish its mission can be significantly affected if it loses the ability to process, retrieve, and protect information that is maintained electronically. For this reason, organizations should have established (1) procedures for protecting information resources and minimizing the risk of unplanned interruptions and (2) plans for recovering critical operations should interruptions occur. A contingency and disaster recovery plan specifies backup operations, emergency response, and postdisaster recovery procedures to ensure the availability of critical resources and facilitate the continuity of operations in an emergency. Such a plan addresses how an organization will deal with a full range of contingencies, from electrical power failures to catastrophic events such as earthquakes, floods, and fires. The plan also identifies essential business functions and ranks resources in order of criticality. To be most effective, a contingency plan should be periodically tested in disaster simulation exercises, and employees should be trained in and familiar with its use.

For fiscal year 1999, the Army Audit Agency identified three control weaknesses related to service continuity and issued corresponding recommendations to address them. The agency reported that the continuity of operations plan for the CEEIS was out of date, and that periodic testing would be needed to identify planning and training deficiencies. It also found that backup tape storage facilities were too close to primary operations centers.[10]

[10]Army Audit Agency, *Corps of Engineers Financial Management System: General and Application Controls*, AA 01-319 (June 26, 2001).

Since the fiscal year 1999 audit, the Directorate of Corporate Information has assumed responsibility for development of service continuity plans for agencywide information systems. A program plan has been drafted for analyzing, defining, and coordinating continuity of operations for the CEEIS. In addition, the Corps is gathering information from functional units to develop a continuity of operations plan that would address the roles of CEFMS and CEEIS in headquarters emergency operations and disaster recovery.

Nevertheless, the weaknesses noted from 1999 in the continuity plans and activities of Corps functional units remained unresolved. The Corps still lacks an overall continuity of operations plan for the CEEIS, and plans for its major processing centers were not yet developed or were incomplete and did not meet federal guidance. Furthermore, the draft program plan to establish a CEEIS continuity of operations plan did not identify the full set of activities required for effective management of this program or establish milestones and performance measures based on recognized federal directives and best practices. The Corps thus lacks effective mechanisms to track the CEEIS service continuity improvement efforts and ensure establishment of integrated plans.

In addition, new weaknesses indicated that the Corps had not effectively managed this area of federal requirements across its functional units. CEFMS obtained interim approval to operate under the Corps' system certification and accreditation process, without detailing the central role of CEEIS in CEFMS service continuity. The Corps' Office of Internal Review found that at least 10 facilities that depend on CEEIS and CEFMS lacked continuity plans for their operations, and 10 more had outdated plans. For example, the Corps did not meet its schedule for obtaining Headquarters service continuity planning information from functional units such as the Directorate of Corporate Information, and it had not yet taken follow-up actions to address this delay to its program.

Persistent weaknesses in service continuity testing are related to inadequacies in continuity of operations plans. No service continuity testing has been conducted for the CEEIS network or for CEFMS, which both lack viable continuity of operations plans. In addition, some existing continuity of operations plans for facilities that rely on CEEIS and CEFMS had not been tested, and no training programs were in place, to ensure that plans could be reliably executed.

Finally, the Army Audit Agency's fiscal year 1999 recommendation to relocate the CEEIS backup storage centers farther away from primary facilities had not been addressed.

Corps officials told us, and these weaknesses confirm, that the Corps lacks a strong focal point for continuity of Corps business operations. Such a focal point is needed to provide agencywide guidance, coordination, integration, and oversight for CEFMS and CEEIS service continuity and disaster recovery planning and preparation. Agencywide management is required to ensure that individual site plans will operate effectively together and to verify that the Corps' response to disruptions will be adequate to support its mission.

The Army Audit Agency plans to issue a report in fiscal year 2002 providing further discussion on these weaknesses.

Network Security Needs Improvement

Network security controls are key to ensuring that only authorized individuals can gain access to sensitive and critical agency data. These controls include a variety of tools, such as user IDs and passwords, that are intended to authenticate and allow authorized users access to the network. In addition, network controls should provide for safeguards to ensure that system software is configured to prevent users from bypassing network access controls or causing network failures.

During our review, we performed preannounced network vulnerability testing, during which we were able to gain access to the Corps' internal network and perform some probing of Corps systems. The access obtained allowed us to map the network, but it did not allow us to gain access to any of the CEFMS production systems. The Corps' intrusion detection team detected our activity and blocked this access once we employed more intrusive techniques.

Our review identified network security weaknesses that could allow unauthorized access to Corps systems; these weaknesses included the following:

Weak logical access controls at the Finance Center. Logical access controls were not adequately implemented to prevent or detect unauthorized individuals with physical access to the facility from gathering sensitive information, such as user IDs and passwords.

Extensive "trust" relationships. The Corps has established trust relationships between network segments to conduct Corps business (CEFMS and non-CEFMS related); however, additional restrictions could be implemented to more effectively control access.

Inadequate restrictions on internal network traffic. The Corps' security model does not employ the control capabilities of certain critical network components to restrict internal network traffic. Consequently, the risk is increased that users could potentially gain unauthorized access to Corps systems.

CEFMS Application Controls Can Be Strengthened

Application controls relate directly to the individual computer programs that are used to perform transactions (such as recording journal entries in the general ledger). In an effective general controls environment, application controls help to ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.

Of the 18 recommendations that we made on application controls in our fiscal year 1999 audit, the Corps had completed action on 13 and had partially completed or was implementing action plans to correct 5. Among the actions taken, the Corps had (for example)

- required electronic signature on updates to the CEFMS access control table;
- changed the CEFMS database design to prevent the same user from paying, certifying, and authorizing certain disbursements and to prevent users from creating and certifying the same invoice for payment; and
- required weekly authorization of disbursing terminals by the Finance Center.

Although the Corps made substantial progress in correcting vulnerabilities, continuing and newly identified vulnerabilities in application computer controls continue to impair the Corps' ability to ensure the reliability, confidentiality, and availability of financial and sensitive data. The numbers in table 2 reflect open recommendations on application controls, including both recommendations remaining from our fiscal year 1999 review and additional recommendations arising from our fiscal year 2001 review.

Table 2: Recommendations by Application Control Area

Area of control	FY 1999 outstanding recommendations	FY 2001 recommendations[a]
Authorization controls	3	6
Accuracy or input controls	1	1
Transaction processing	0	0
Electronic signature	1	0
Total	**5**	**7**

[a]These include recommendations on two weaknesses that were corrected during our fieldwork.

Authorization Controls Were Not Adequate

Like general access controls, access controls for specific applications should be established to ensure that (1) only authorized transactions are entered into the application, (2) duties are properly segregated and individuals can be held accountable, and (3) modifications to user access permissions are authorized and audited.

In some instances, proper authorization controls were not enforced, as in the following examples.

- User access permissions in CEFMS did not match authorized access request forms, thereby increasing the risk that a user could process CEFMS transactions that were not authorized or consistent with management's intent.

- Electronic signature header records[11] were still not being routinely reviewed and analyzed to detect whether individuals were performing incompatible duties associated with critical transactions; this increased the risk that unauthorized transactions would go undetected.

- CEFMS development personnel had user IDs allowing them to generate invoices at other locations, thereby increasing the risk of inappropriate activity.

[11]Electronic signature transactions generate a header record every time a user signs a transaction. The header information includes information such as the user ID of the person signing the transaction and the date and time the transaction was signed.

- User transactions processed on the disbursing terminals were not subject to postpayment audits. This situation increases the risk that a malicious user could input fraudulent transactions without detection.

Documentation of Input Controls Was Not Current

For an application system to produce reliable results, the data input to the system must be valid and accurate. Input controls include

- well-designed data entry,
- data validation and editing to identify and correct erroneous data,
- automatic reporting of erroneous data, and
- review and reconciliation of output.

CEFMS user manuals pertaining to the work management module do not reflect current information, including up-to-date input controls. The Corps has determined the manual to be obsolete and is performing a functional review. Outdated manuals increase the risk that employees may follow input procedures that are inadequate or improper.

Electronic Signature Capabilities Were Not Adequately Used

To identify users associated with certain types of transactions, CEFMS uses an electronic signature system. The Corps requires the use of the electronic signature system for CEFMS transactions that lead to an obligation, collection, or disbursement of government funds. The electronic signature system consists of a smartcard, smartcard reader, cryptographic module, and central database containing all system user IDs. The electronic signature system was designed to provide assurance that a document signed by an authorized person has not been altered. This assurance relies on Corps policy, which assumes that the electronic signature smartcard has only been used by the individual to whom it was issued.[12]

We previously reported that the Corps had not adequately used CEFMS electronic signature capabilities to help ensure data integrity for certain

[12]Users who electronically sign documents accept the same responsibility as when signing documents by hand. We outlined the necessary attributes of electronic signatures in *Corps of Engineers Electronic Signature System*, GAO/AIMD-97-18R (Washington, D.C.: November 19, 1996), and in Comptroller General Decision 71 Comp. Gen. 109 (1991).

transactions. For the 35 percent of CEFMS functions[13] for which electronic signature verification is required, alterations of data would be detected during transaction processing. However, for some sensitive functions, use of the electronic signature system was not required, including some functions that were financial transactions (such as general ledger journal authority). Such "unsigned" records could be added, modified, or deleted without detection. The Corps had not reevaluated the CEFMS functions to determine whether other sensitive transactions should require electronic signature.

During the fiscal year 2001 audit, several instances were identified of CEFMS users sharing their CEFMS electronic signature smartcards with other Corps employees. One critical requirement in implementing the electronic signature system was that each smartcard be under the sole control of an individual smartcard holder. However, according to tests performed by the Army Audit Agency at one Corps site, card sharing had occurred. As a result, authentication controls were not effective to provide reasonable assurance that users' electronic signatures are valid. Consequently, the Corps cannot ensure that its electronic signature system authenticates transactions and mitigates other computer control weaknesses identified in CEFMS. To help maintain the integrity and security of CEFMS, the Corps issued a memorandum on January 17, 2002, reinforcing the need to comply with Army and Corps policies that prohibit sharing of electronic signature cards and passwords. The Army Audit Agency is continuing to review the effectiveness of authentication controls over CEFMS electronic signature card users. The agency plans to issue a separate report to Corps management during fiscal year 2002.

Conclusions

Information system general and application controls are critical to the Corps' ability to manage its computer security and to ensure the reliability, confidentiality, and availability of its financial and sensitive data. While the Corps has made substantial progress in resolving many of the fiscal year 1999 weaknesses that we identified and has taken other steps to improve security, continuing and newly identified weaknesses were identified in the Corps' information system control environment. Specifically, at the general

[13]CEFMS functions consist of 109 types of user access that are needed to perform various transactions included in the CEFMS application modules. Of the 109, 38 require electronic signature capability. These functions include those associated with disbursing authorization, district security officer, travel authenticating official, etc.

controls level, the Corps had not adequately (1) limited user access; (2) developed adequate system software controls to protect programs and sensitive files; (3) documented software changes; (4) segregated incompatible duties; (5) addressed service continuity needs; and (6) secured network access. At the application control level, the Corps had not maintained current and accurate CEFMS access authorizations and maintained CEFMS current user manuals. The weaknesses that we identified at the two data processing centers and other sites placed the Corps' computer resources, programs, and files at risk from inappropriate disclosure of financial and sensitive data and programs, modification of data, misuse of or damage to computer resources, or disruption of critical operations.

A primary reason for the Corps' information system control weaknesses was that it had not yet fully developed and implemented a comprehensive security management program. A comprehensive program for computer security management is essential for achieving an effective general and application controls environment. Effective implementation of such a program provides for (1) periodically assessing risks, (2) implementing effective controls for restricting access based on job requirements and actively reviewing access activities, (3) communicating the established policies and controls to those who are responsible for their implementation, and (4) evaluating the effectiveness of policies and controls to ensure that they remain appropriate and accomplish their intended purpose.

Recommendations

In our March 15, 2002, "Limited Official Use Only" report, we recommended that you instruct the chief information officer and the deputy chief of staff for resource management to implement corrective actions to resolve the general and application computer control weaknesses that we identified in that report.

In its report on the Corps' entitywide security management and service continuity, planned for fiscal year 2002, the Army Audit Agency plans to address recommendations in these areas.

Agency Comments

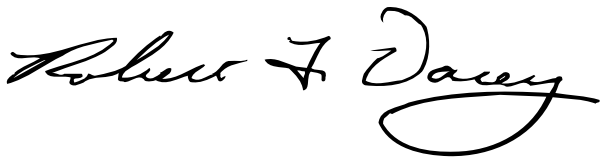
In providing written comments on a draft of this report, the commanding general of the U.S. Army Corps of Engineers agreed with our findings and recommendations and stated that the numerous working meetings

concerning the information security weaknesses that we identified will help expedite their corrective actions. His comments are reprinted in appendix I of this report. The commanding general also stated that the Corps has already completed corrective action on 11 of the open fiscal year 1999 and the new fiscal year 2001 recommendations. The Corps has developed an action plan to correct all but 12 of the remaining recommendations by September 30, 2002, and stated that these 12 recommendations would be completed by fiscal year 2003 or beyond.

We are sending copies of this report to the Senate Committee on Armed Services; the Senate Committee on Governmental Affairs; the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, House Committee on Government Reform; the House Armed Services Committee; the under secretary of defense (comptroller/chief financial officer); the assistant secretary of defense (command, control, communications & intelligence); the deputy inspector general, Department of Defense; the assistant secretary of the army (financial management and comptroller); the director of information systems for command, control, communication, and computers; army auditor general; the deputy chief of staff operations and plans; the deputy chief of staff for intelligence; and the commander, U.S. Army Intelligence and Security Command. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you have any questions regarding this report, please contact me at (202) 512-3317. Key contributors to this assignment were Lon Chin, Barbara Collier, Edward M. Glagola, Jr., David Hayes, Harold Lewis, Paula Moore, Duc Ngo, Eugene Stevens, Crawford L. Thompson, and Jenniffer F. Wilson.

Sincerely yours,



Robert F. Dacey
Director, Information Security Issues

Comments from the U.S. Army Corps of Engineers

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

REPLY TO
ATTENTION OF:

Office of Internal Review

MAY 2 0 2002

Mr. Robert F. Dacey
Director
Information Security Issues
U.S. General Accounting Office
441 G Street NW
Washington D.C. 20548

Dear Mr. Dacey:

The U.S. Army Corps of Engineers reviewed your draft report, subject: Information Security: Corps of Engineers Making Improvements, but Weaknesses Continue (GAO-02-589, April 2002) and provides the following command response.

The numerous pre-report working meetings between our staffs concerning identified security issues did much to improve the overall audit process, enable us to concur with the recommendations, and will hasten our corrective actions. Many of your report recommendations deal with new computer security areas reviewed by this report. Since completion of your audit field work, our corrective actions have been completed on 11 of the 93 carried forward and new audit recommendations. We plan to complete the corrective actions on most of the open issues by 30 September 2002 and 12 actions carry forward to FY 03 and beyond. Further technical discussions between our staffs will be necessary as the planned corrective actions take place.

The U.S. Army Audit Agency under the Chief Financial Officers Act (CFO) for FY 01 recently issued the Corps a qualified audit opinion on its Civil Works program Balance Sheet. Therefore, we look forward to your FY 02 follow-on audit since the results of your computer security audit must be considered by the CFO auditor when opining on the Civil Works FY 02 Statement of Net Costs, Changes in Net Position, Budgetary Resources, and Financing.

Sincerely,

Robert B. Flowers
Lieutenant General, USA
Commanding

GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00