United States General Accounting Office

GAO

Report to the Acting Commander,
U.S. Army Corps of Engineers

October 2000

FINANCIAL MANAGEMENT

Significant Weaknesses in Corps of Engineers' Computer Controls

GAO-01-89

GAO
Accountability * Integrity * Reliability

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

October 11, 2000

Major General Russell L. Fuhrman, USA
Acting Commander
U.S. Army Corps of Engineers

Dear General Fuhrman:

In connection with fulfilling our requirement to audit the annual U.S. government consolidated financial statements,[1] we reviewed general and application controls over the U.S. Army Corps of Engineers' systems. On September 15, 2000, we issued a "Limited Official Use" report to you detailing the results of our review. This version of the report for public release summarizes the vulnerabilities we identified and the recommendations we made.

This report presents the results of our tests of the effectiveness of general and application controls that support the Corps' key financial system. This system processes military engineering, construction, and real estate projects and civil works projects involving the investigation, development, and maintenance of the nation's waters and related environmental resources. While performing our work, we made the results of our review available to the Department of Defense (DOD) Office of Inspector General and the Army Audit Agency for its use in performing the required fiscal year 1999 financial statement audit of the U.S. Army Corps of Engineers, Civil Works. We also communicated our findings to Corps' management. This report provides an overall assessment and summary of Corps' computer control vulnerabilities and recommendations we made. The Corps' comments are discussed in the "Agency Comments and Our Evaluation" section of this report and are reprinted in appendix I.

Results in Brief

The pervasive weaknesses that we identified in Corps' computer controls at its data processing centers and other Corps' sites revealed serious vulnerabilities that would allow both hackers and numerous legitimate users with valid access privileges to improperly modify, inappropriately disclose, and/or destroy sensitive and financial data, including Privacy Act data such as social security numbers and other personal information.

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

Further, such weaknesses could result in a disruption of critical computer-based operations. These weaknesses also increase the vulnerability of other DOD networks and systems to which the Corps' network is linked. As a result of these weaknesses, we consider computer security over the Corps' financial system to be ineffective.

Serious general control weaknesses impaired the Corps' ability to protect computer resources, limit access to computer programs and files, control powerful systems software, ensure that only authorized programs were placed in operation, and enforce proper segregation of duties. In addition to the general control weaknesses that we identified, the Army Audit Agency determined that the Corps did not have an effective entitywide security management program or continuity of operations plan. These weaknesses affect the Corps' ability to (1) adequately assess computer risks and monitor and evaluate the effectiveness of security procedures and (2) protect information resources and minimize the risk of potential disruptions, such as temporary power failures, natural disasters, and malicious attacks.

Also, we found significant application control weaknesses related to the authorization and recertification of access, updates to the access control table,[2] the assignment of responsibilities, and the assignment and protection of electronic signature cards. These weaknesses could, for example, result in (1) user activity that is not consistent with Corps' security objectives, management's authorized intent, or user job responsibilities, (2) fraudulent financial reporting, such as the misuse of inventory adjustments, labor cost transfers, and general ledger transactions, (3) a single individual gaining control of a transaction from initiation to completion, and (4) an individual entering a fraudulent transaction in the financial system, such as by accessing an unattended terminal with an electronic signature card left in the reader and attributing that transaction to another user.

These general and application control weaknesses impair the Corps' ability to ensure the confidentiality and availability of data contained in the financial system. Additionally, although the financial system has the capability to validate the integrity of electronically signed transactions, the general and application control weaknesses that we identified impaired the

[2]The financial system access control table is the table whereby user permissions from the financial system access request forms are entered.

effectiveness of the electronic signature technology. We also found weaknesses related to the Corps' use of the electronic signature capabilities. For example, certain sensitive functions were not protected by the electronic signature technology, and the Corps did not have an effective process for periodically revalidating the integrity of already signed data stored in the database for financial reporting or other financial management use.

Our "Limited Official Use" report included a total of 93 recommendations that will help strengthen and improve general and application controls and the Corps' implementation and use of electronic signature capabilities. These recommendations include those designed to protect computer resources against unauthorized access to financial and sensitive programs and data, strengthen system security, improve control procedures for software changes, ensure adequate segregation of duties, improve application controls, and effectively use electronic signature capabilities.

In commenting on a draft of this report, the Acting Commander of the U.S. Army Corps of Engineers agreed that there are weaknesses in the Corps' systems, including weaknesses in access control, application software development and change control, systems software, segregation of duties, and application control. The Corps stated that it had already corrected some of the issues and was acting to correct many others promptly. However, the Corps did not agree with 13 of our 93 recommendations or our overall assessment of the extent of its computer security problems. Given the importance of the individual control issues, we continue to believe that implementing these recommendations would enhance the Corps' overall security environment. Further, the widespread nature of the weaknesses we identified along with the Corps' lack of an overall security management plan clearly reflects the existence of pervasive weaknesses in the Corps' security infrastructure.

Background

The Corps has both a military and civil works mission. The Corps' military mission involves managing and executing engineering, construction, and real estate programs for the U.S. Army and Air Force, other federal agencies, state and local governments, and foreign governments. The Corps also provides military support to its customers by managing and executing Army installation support programs, developing and maintaining the capability to mobilize in response to national security emergencies, and supporting Army space initiatives. The Corps' civil works mission involves

investigating, developing, and maintaining the nation's water and related environmental resources.

The Corps receives appropriated funds for military programs and civil works. Additionally, the Corps receives funds from nonfederal entities (local municipalities and state governments) for civil projects. The Corps also has a revolving fund for common services that apply to multiple projects. The financial system integrates all of the Corps' major business processes, including cost accounting, disbursing, billing, and financial management reporting. The financial system supports about 63 Corps sites, including 4 regional centers, 8 divisions, and 41 districts. A separate financial statement is prepared for Corps of Engineers, Civil Works, activities. The Corps' military activities are included in the Department of the Army's financial statements.

The financial system uses an electronic signature system intended to identify the user associated with a given transaction. Processing transactions that lead to the obligation, collection, or disbursement of government funds require the use of the electronic signature system. About 36 percent of the financial system functions require the use of the electronic signature system. The electronic signature system is an integral part of the financial system's workflow process. As a transaction processes through its life cycle, the electronic signature system is used to verify that data have not been altered. Specifically, when a transaction requiring electronic signature verification is first entered into the financial system, an electronic signature is generated that links the data to the user. When the transaction proceeds to the next user for action, before it appears on the computer screen, the electronic signature system validates that none of the data that were signed by the previous user have been changed. Therefore, if any alterations occur, the electronic signature system provides reasonable assurance that the alteration will be detected before the next user acts upon the transaction.

The financial system, a database application, processes the financial data at the Corps' data processing centers. Each Corps site maintains its own database and provides its financial data to be processed at one of the data processing centers.

Objective, Scope, and Methodology

Our objective was to evaluate and test the effectiveness of selected computer controls over the Corps' financial system in connection with the Army Audit Agency's fiscal year 1999 U.S. Army Corps of Engineers, Civil

Works, financial statement audit. We contracted with an independent public accounting firm, PricewaterhouseCoopers, LLP, to assist in the evaluation and testing of the financial system computer controls. We determined the contractor's scope of audit work and monitored its progress. To rely on the work of the contractor, we

- evaluated the qualifications and independence of the staff;
- reviewed and approved the contractor's approach, plans, and work programs;
- attended key meetings between the contractor and Corps personnel;
- monitored technical testing; and
- reviewed the contractor's working papers to determine whether evidence in the working papers supported the contractor's findings.

The contractor used our *Federal Information System Controls Audit Manual* (FISCAM) to guide the general controls testing, which included four of the six FISCAM general control sections: (1) Access Controls, (2) Application Software Development and Change Control, (3) Systems Software, and (4) Segregation of Duties. The Army Audit Agency performed tests on the two remaining FISCAM sections: entitywide security management program and service continuity. During fiscal year 2000, the Army Audit Agency issued a report to the agency head and an individual report to each Corps site where it tested these two FISCAM sections.

To evaluate general computer controls, the contractor identified and reviewed the Corps' information system policies and procedures related to general controls, conducted tests, observed controls in operations, and interviewed cognizant Corps officials.

The contractor performed external vulnerability testing on the Corps' Internet gateways, internal vulnerability testing at the Corps' data processing centers and one Corps District, and dial-in vulnerability testing from a list of Corps telephone numbers. Through the vulnerability testing, the contractor attempted to gain access to Corps' servers by guessing valid user names and passwords and by using other hacker tools and techniques. These attempts were performed with the knowledge and cooperation of Department of Defense, Department of the Army, and U.S. Army Corps of Engineers officials.

To evaluate and test application controls over selected system modules, the contractor used a proprietary methodology tailored to the financial system. Specifically, the contractor tested

- access controls,
- input controls,
- data processing controls,
- rejection controls, and
- output controls.

The financial system modules tested were: work management, resource plans, funding, purchase request and commitments, obligations, expenditures, disbursements, bill and collect, asset management, and labor processing.

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. We plan to perform a follow-up review of these matters.

Our general and application control testing was performed from September 1999 through January 2000. We performed our work at the Corps' data processing centers and other Corps sites. Additionally, we held interviews with cognizant officials at Corps headquarters, located in Washington, D.C. Our work was performed in accordance with generally accepted government auditing standards.

General Computer Control Weaknesses Place Corps Data at Significant Risk

General controls are the structures, policies, and procedures that apply to an entity's overall computer operations. General controls establish the environment in which application systems and controls operate. An effective general control environment would

- ensure that an adequate computer security planning and management program is in place;
- protect data, files, and programs from unauthorized access, modification, and destruction;
- limit and monitor access to programs and files that control computer hardware and secure applications;
- prevent unauthorized changes to systems and applications software;
- prevent any one individual from controlling key aspects of computer-related operations; and
- ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption.

Our fiscal year 1999 review of general computer controls over Corps' systems identified weaknesses in access controls, systems software, application software development and change controls, and segregation of duties. In addition, the Army Audit Agency's fiscal year 1999 review of the Corps' security management program and service continuity of operations plan identified control weaknesses.

Access Controls

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

Logical access controls involve the use of computer hardware and security software programs to prevent or detect unauthorized access by requiring users to input unique user identifications, passwords, or other identifiers that are linked to predetermined access privileges. Logical security controls restrict the access of legitimate users to the specific systems, programs, and files they need to conduct their work and prevent unauthorized users from gaining access to computing resources.

Physical security controls include locks, guards, badges, alarms, and similar measures (used alone or in combination) that help to safeguard computer facilities and resources from intentional or unintentional loss or impairment by limiting access to the buildings and rooms where they are housed.

The Corps did not have effective access controls. The Corps did not (1) adequately control remote access to the Corps' processing environment, (2) protect network devices, (3) limit powerful access privileges to only those users who needed such access to perform their duties, (4) monitor access paths to the relational database, (5) have strong password controls, and (6) use database auditing features to detect and monitor security violations. These weaknesses are illustrated by the following examples.

- Remote access to the Corps' processing environment was not sufficiently controlled, thereby providing inadequate protection from unauthorized access by intruders.
- Weak passwords in the network control devices allowed remote read/write access, thereby increasing the risk of unauthorized

monitoring and capturing of all network traffic and using that information to launch further attacks.

- A large number of users were erroneously granted access to powerful privileges and had the capability to perform database functions that they were not authorized to perform, thereby increasing the risk that data contained in the financial system could be altered by either a direct connection to the database or by a user changing his or her application access permissions in the access control table.
- Logging and monitoring individuals' access to data stored on the financial system, particularly access to nonstandard user accounts and accounts with special privileges, did not occur routinely, thereby increasing the risk that sensitive data and programs were not protected and controlled.
- Weak password management allowed user names and passwords to be successfully guessed during vulnerability testing, thereby increasing the risk that a user could gain unauthorized access to Corps' systems.
- Audit logs were not used to detect and monitor security violations, thereby increasing the risk that violations could continue to occur undetected.

Systems Software

Systems software coordinates and helps control the input, processing, output, and data storage associated with all of the applications that run on a system. Systems software includes operating system software, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems. Controls over access to and modification of system software are essential to protect the overall integrity and reliability of information systems.

Our review of systems software controls identified weaknesses related to (1) disclosure of financial and sensitive information over the Internet, (2) vulnerabilities in operating system configurations, and (3) ineffective security controls over Corps' servers. These weaknesses are illustrated by the following examples.

- Vulnerabilities in system configuration allowed financial and sensitive information, including Privacy Act data, to be accessed from over the Internet, thereby increasing the risk that unauthorized users could electronically impersonate many employees or misuse information. During vulnerability testing, we gained access to a prior-year database backup file containing financial and sensitive information and an

archive database containing all of the 1999 fiscal year-end financial information. The vulnerabilities in the operating system configuration could allow an unauthorized user the ability to modify, read, download, or delete the information from these database files.

- A vulnerability in the operating system configuration, which allowed unauthorized system administrator-level access, existed on the Corps' computer that centrally stores critical electronic signature system information. This vulnerability increased the risk that an attacker could delete information used to verify electronic signatures and, therefore, cause a disruption of critical computer-based operations. In November 1999, the contractor gained access to this computer during its vulnerability testing of the network. The Corps took immediate action to disable the function that allowed the unauthorized attack.
- Servers allowed unauthenticated connections (connections that were possible without a user name and password), 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.

Application Software Development and Change Controls

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 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 and processing irregularities or malicious code from being introduced.

Our review of application software development and change controls at the development site for the financial system determined that improvements were needed over application software development and change control procedures specific to emergency changes, test acceptance, and problem reporting. We also found that Corps' employees took home backup tapes containing the financial system production code and did not use a log to document the location of the backup tapes. These weaknesses increased the risk that users could make unauthorized or erroneous changes to a program in production and backup tapes may not be usable or available for recovery efforts.

Segregation of Duties

Another key control for safeguarding programs and data is to ensure that duties and responsibilities for authorizing, processing, recording, and reviewing data, as well as initiating, modifying, migrating, and testing of

programs, are separated to reduce the risk that errors or fraud will occur and go undetected. Duties that should be segregated from one another include application programming and system programming and responsibilities for computer operations, security, and quality assurance.

We found that controls within the information management functional areas at the Corps' data processing centers needed improvement. For example, the Corps lacked formal policies and procedures for monitoring and documenting which job functions are incompatible, thereby increasing the risk that incompatible duties are being performed by the same individuals or that systems resources could be altered, damaged, or destroyed.

We also identified other segregation of duties control weaknesses during our review of access controls. For example, physical security controls at the Corps' data processing centers needed improvement. In particular, we found that users at the data centers with card-key access could access all areas within the data centers, including the master operations consoles for the financial system application, an area that should generally be limited to network operations staff. Also, at one data center, several employees without justified business or job-related purposes had unrestricted access to computer facilities.

Results of the Army Audit Agency's Computer Control Work

The general and application control weaknesses that we identified are symptomatic of an ineffective security management program. An effective program would include implementing guidance that established appropriate policies and related controls, raising awareness of prevailing risks and mitigating controls, and monitoring and evaluating the effectiveness of established controls. Work performed by the Army Audit Agency indicated that the Corps did not comply with applicable federal, DOD, and Army regulations pertaining to security management and continuity of operations. Specifically, the Corps did not have a comprehensive security management program or a current service continuity of operations plan. The Corps' risk assessment and security plan was outdated, a formal incident response team was not in place to effectively respond to computer security threats, and the mandatory computer security training program was not adequate. The Corps' continuity of operations plan was not periodically tested, did not consider possible scenarios in case of a natural or man-made disaster, did not address the current workload, and did not reflect the current hardware

configuration. The Army Audit Agency will be issuing a separate report providing more detail on its findings.

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 control environment, application controls help to further ensure that transactions are valid, properly authorized, and completely and accurately processed and reported. The application control weaknesses that we identified in access, accuracy, and processing controls, in addition to the general control weaknesses, further weaken the financial system's control environment.

Access Controls

Like general access controls, access controls for specific applications should be established to (1) ensure that only authorized transactions are entered into the application, (2) ensure individual accountability and proper segregation of duties, and (3) ensure that modifications to user access permissions are authorized and audited.

Access control weaknesses noted in our review included the following.

- The financial system's access request forms were missing, unapproved, or inaccurate, thereby increasing the risk that a user could process transactions in the financial system that are not authorized or consistent with management's intent.
- The lack of audit trails and security controls over updates made to the financial system's access control table increased the risk that users could change their access permissions and potentially gain control of a transaction from initiation to completion without the involvement of or subsequent review by a third party. However, users who did not have electronic signature cards could only change their access permission to perform transactions that did not require an electronic signature.
- The lack of routine tests of information contained in the header records[3] to detect whether segregation of duties controls were being circumvented increased the risk that unauthorized transactions would not be detected by management. The financial system's access control

[3]A header record is a secure record that contains information, such as the user who signed a transaction, and is generated by the electronic signature system each time a user signs a transaction.

table prevents a user from being simultaneously assigned functions that would create a segregation of duties problem. However, because of weaknesses discussed previously with the access control table, the financial system did not prevent a user from performing incompatible functions if the functions were assigned at separate times. At our request, the Corps developed a program during the audit that can be used to determine whether any transactions signed by the electronic signature system and recorded in the financial system would present a segregation of duties problem.

We also found that controls over the use of electronic signature cards and disbursing terminals could be improved as illustrated by the following.

- Electronic signature cards remained active on the financial system's terminals for up to 90 minutes of user inactivity.
- System administrators were not reviewing access to terminals authorized for funds disbursement often enough to provide optimal oversight and control.
- Multiple electronic signature cards were issued to certain users, some of which would allow incompatible functions to be performed.

Weaknesses in the use of electronic signature cards and disbursing terminals increase the risk that fraudulent or unauthorized transactions could be entered without detection or that controls designed to prevent a user from performing incompatible duties could be circumvented.

Input Controls

The recording of valid and accurate data into application systems is essential to provide for an effective system that produces reliable results. Accuracy or input controls include

- well-designed data entry;
- data validation and editing to identify erroneous data;
- reporting, investigating, and correcting erroneous data; and
- reviewing and reconciling output.

We found that user manuals for the financial system were outdated and inaccurate, and the financial system's edit controls pertaining to input of transaction dates required improvement. Manuals that do not reflect accurate or current information increase the risk that employees may perform inadequate or improper procedures. Edit controls that do not include a check for reasonableness of transaction dates increase the risk

that information could be reported inaccurately or omitted in a given accounting or reporting period.

Controls Over Data Processing

Controls over data processing are designed to ensure that data are processed completely, accurately, and promptly. As a result of data processing tests performed on the financial system production databases, we identified potential data anomalies. For example, each work item, or project, is assigned an employee to manage and control the project costs, and the data field in the table should be filled in with the employee's identification number. However, this data field was blank for 8,639 of the 75,284 records examined. We were unable to determine the specific causes of data anomalies and recommended in our Limited Official Use report that the Corps (1) determine the causes of erroneous data existing in the financial system, (2) eliminate those causes as appropriate, and (3) correct existing erroneous data.

Use of Electronic Signature Capabilities

We also found that the Corps did not adequately use electronic signature capabilities to help ensure data integrity for certain transactions. For the 36 percent of system functions that are subject to electronic signature verification, alterations of data would be detected during transaction processing. However, the electronic signature system was not used to validate sensitive functions, including some financial transactions, such as general ledger journal authority and year-end closings. Due to the pervasive weaknesses described previously, "unsigned" records could be added, modified, or deleted without detection. Further, the Corps did not use the electronic signature system to revalidate the integrity of electronically signed records that were no longer active and were contained in the database for later use, such as data used to prepare year-end financial reports. This inactive period could permit data to be altered and, without revalidation prior to use, such alterations may not be detected. We did not verify the integrity of electronically signed transactions in the database.

Conclusions

As a result of the pervasive weaknesses that we identified in the Corps' computer controls, including its two data processing centers, the Corps' overall computer control security was not effective. The Corps did not have a reliable set of computer controls to help ensure the confidentiality, availability, and integrity of financial and sensitive data contained in the financial system. Although the Corps implemented an electronic signature

system in its financial system to help ensure data integrity and to detect improper actions, serious weaknesses in Corps' computer security impaired the effectiveness of the electronic signature technology. Because the financial system provides users with access to significant amounts of financial data and computer resources, well-designed and effective general and application controls are essential if Corps' operations, programs, files, and facilities are to be properly protected. These weaknesses are symptomatic of the lack of an effective security management program, in which computer risks are adequately assessed and security procedures are monitored and evaluated for their effectiveness. A significant and sustained commitment by Corps' management will be necessary to fully address these significant computer control weaknesses.

Recommendations

In our September 15, 2000, "Limited Official Use" report, we recommended that you direct and determine that the Deputy Chief of Staff for Resource Management, along with the Chief Information Officer, implement corrective actions to resolve the general and application computer control weaknesses that we identified in that report.

Agency Comments and Our Evaluation

In commenting on a draft of this report, the Acting Commander of the U.S. Army Corps of Engineers agreed that the Corps has weaknesses in its systems, specifically access control, application software development and change control, systems software, segregation of duties, and application control. However, the Corps stated that it disagrees with many of the issues, and that some of these issues are not workable or affordable, although its comments did not provide specific support for its view. In the Corps' detailed response to our "Limited Official Use" report, these areas of disagreement cover about 13 of the 93 recommendations. As a result of a July 25, 2000, meeting with Corps infrastructure and information management officials, we clarified the intent of these 13 recommendations to more precisely reflect the needed management and technical initiatives. If properly implemented, these recommendations would ensure that computer networks, data, and resources are restricted to legitimate users; job functions related to information management are adequately segregated; and data contained in the Corps' financial system are accurate and complete. Given the importance of these individual control issues, we continue to believe that implementing these recommendations would enhance the Corps' overall security environment.

Also, from an overall perspective, the Corps did not agree with our assessment of the extent of its computer security problems. Specifically, the Corps disagrees that it has pervasive weaknesses and states that its use of electronic signature technology provides added security. We continue to believe that our characterization of the weaknesses is appropriate. The results of our review showed that the Corps has serious weaknesses in several functional categories. Also, as stated in our report, the general and application control weaknesses that we identified impaired the effectiveness of controls associated with individual applications, such as the electronic signature system. Further, the widespread nature of the weaknesses we identified along with the Corps' lack of an overall security management plan clearly, in our judgment, reflect the existence of pervasive weaknesses in the Corps' security infrastructure.

The Corps is developing a corrective action plan to address many of the weaknesses identified. However, the Corps stated that it needed specific input as to which issues it should focus on in executing its corrective action plan. We previously discussed our assessment of the high-risk weaknesses with Corps officials and believe we provided the specific input that is again being requested. If needed, we will meet with the Corps to discuss these matters further.

We would like to emphasize one important issue; as stated in our "Limited Official Use" report, our audit was not designed to test all controls and, therefore, the computer control weaknesses that we identified, while very serious, are not all inclusive. Also, because the Corps' computer environment is constantly changing, new weaknesses may occur. Therefore, we emphasized that Corps' efforts in correcting the weaknesses should be institutionalized as part of a continuing cycle of risk management activity. As stated in our report, these practices fall under the framework of an effective security management program. An effective security management program would include establishing a process and assigning responsibility for systematically assessing risk, developing and implementing effective security policies and controls, and monitoring the appropriateness and effectiveness of these policies and related controls.

We are sending copies of this report to Senator Fred Thompson, Senator Joseph Lieberman, Representative Floyd Spence, Representative Ike Skelton, Representative Dan Burton, Representative Henry A. Waxman, Representative C.W. Bill Young, Representative John P. Murtha, Representative Tillie Fowler, and Representative James A. Traficant, Jr., in

their capacities as Chairmen or Ranking Minority Members of Senate or House Committees and Subcomittees. We are also sending copies of this report to William J. Lynn, Under Secretary of Defense (Comptroller/Chief Financial Officer); Arthur L. Money, Assistant Secretary of Defense (Command, Control, Communications and Intelligence); Donald Mancuso, the Office of Inspector General, Department of Defense; Helen McCoy, Assistant Secretary of the Army (Financial Management and Comptroller); Lieutenant General William H. Campbell, Director of Information Systems for Command, Control, Communication, and Computers; Francis E. Reardon, The Auditor General of the Army; Lieutenant General Larry R. Ellis, Deputy Chief of Staff Operations and Plans; Lieutenant General Robert W. Noonan, Jr., Deputy Chief of Staff for Intelligence; and Colonel Donald Woolfolk, Acting Commander, U.S. Army Intelligence and Security Command. Copies will be made available to others upon request.

If you have any questions regarding this report, please contact me at (202) 512-9095. Key contributors to this assignment are listed in appendix II.

Sincerely yours,

Lisa G. Jacobson
Director
Financial Management and Assurance

Comments From the 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

29 SEP 2000

Mr. Jeffrey C. Steinhoff
Assistant Comptroller General
Accounting and Information Management
Division
U. S. General Accounting Office (GAO)
Washington, D.C. 20548

Dear Mr. Steinhoff:

The U.S. Army Corps of Engineers reviewed your draft report, subject: Corps of Engineers Computer Control Weaknesses (GAO/AIMD-00-320) and is providing the following command response. An interested party needs to know that you plan to perform follow-on audit work using Pricewaterhouse Coopers (PwC). We believe it is premature to issue this report because: (i) there has not been a resolution of the many issues on which we disagree; (ii) credit cannot not be given to the corrective actions already taken since the PwC follow-on audit has not occurred; (iii) certain agreed upon corrective actions will take longer than 1 October 2000 to implement; and (iv) we would still like to have your input as to which of the 34 issues and 93 recommendations are critical to our FY 2001 Chief Financial Officer Act (CFO) audit opinion so we can better focus our corrective action effort.

The PwC audit identified some viable access control, application software development and change control, systems software, segregation of duties, application input controls, and processing controls system weaknesses. However, certain audit issues are not workable or affordable in the current USACE resource environment. We have already corrected some issues and we are moving forward to correct many others in a timely manner. However, there are key issues that we disagree with and others which require a corrective action period that extends into Fiscal Year 2001. From our responses to your "Limited Official Use Only" report, you already know, both verbally and in writing, the corrective actions taken or underway, why we disagree with certain results and recommendations, and our overall report concerns. It would be difficult to reiterate them in this letter because of their sensitivity and number of issues. A preliminary working meeting was held in January and another held in July after issuance of the draft report. The issues on which we differ were discussed. Some progress was made to resolve our differences but more meetings are needed.

In summary, I am of the opinion that the Corps is working hard to comply with our governing policy, Army Regulation (AR) 380-19. The Corps of Engineers automated systems are continually being modernized and security strengthened. Therefore, we do not believe we have "pervasive weaknesses" as stated throughout the report. We are at the technology forefront in the use of electronic signatures to provide added security. This is a costly control so it must be judiciously applied where it is cost effective. The PwC report addresses many conceptual Corps security weaknesses, yet external audit reports issued concerning our financial transactions have not identified corrupted financial data. We are working hard to provide the government and our customers with a safe and secure information system and financial management operating system. I currently have my internal audit staff doing work in all our districts on many of the issues identified by PwC.

Sincerely,

for Milton Hunter MG, USA
Russell L. Fuhrman
Major General, U.S. Army
Acting Commander

Staff Acknowledgments

Cleggett S. Funkhouser, Jenniffer F. Wilson, Edward M. Glagola, Jr., David B. Hayes, Crawford L. Thompson, and Sharon S. Kittrell made key contributions to this report.

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

***Orders by visiting*:**
Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

Orders by Internet:
For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, or Abuse in Federal Programs

Contact one:

- **Web site: http://www.gao.gov/fraudnet/fraudnet.htm**
- **e-mail: fraudnet@gao.gov**
- **1-800-424-5454 (automated answering system)**

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

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Rate
Postage & Fees Paid
GAO
Permit No. GI00