

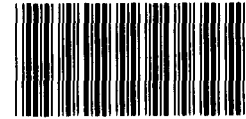


United States  
General Accounting Office  
Washington, D.C. 20548

Information Management and  
Technology Division

B-251454

December 14, 1992



148127

Mr. Dallas L. Peck  
Director  
U.S. Geological Survey

Dear Mr. Peck:

We recently tested the use of an automated auditing software package, Expert Auditor, to assess technical and operational security controls of the National Earthquake Information Service's Seismic Data Analysis System (SEDAS). This test, which was conducted in cooperation with the Geological Survey, was valuable in helping us to assess how well this software worked. In addition, the test yielded some information about SEDAS security that you might find useful. This letter describes the results of our audit of SEDAS using Expert Auditor. Details of our objective, scope, and methodology are discussed in enclosure I

SEDAS is a mission-critical system that provides information on the location of earthquakes to the academic community, the private sector, and to other government agencies throughout the U.S. and the world. This information is used to trigger rapid deployment of rescue teams and resulted in saving thousands of lives in the recent earthquakes in Romania and Iran.

SECURITY CONTROLS ARE GENERALLY ADEQUATE

SEDAS, in most respects, has adequate safeguards and controls in place to mitigate many of the security risks, such as loss of data and availability of service, associated with automation. Officials responsible for managing and operating the system were generally knowledgeable of computer security issues. These officials have appropriately put in place a variety of technical security controls, including passwords, backups, access controls, and physical security controls, to protect SEDAS and its computer resources. Although we identified security weaknesses concerning privacy data,

GAO/IMTEC-93-10R, Geological Survey: Computer Security

856064/148127

training, access control, and password management, Geological Survey officials have already taken or plan to take appropriate steps to correct these weaknesses (see enclosures IV through VII).

CONTINGENCY PLAN IS NOT EFFECTIVE

We were primarily concerned with the effectiveness of SEDAS' contingency plan, which outlines how system operations would be continued if the main computing site was disabled. The existing contingency plan appropriately identifies an alternate site at which operations could be continued. However, the contingency plan does not address how seismic data would be communicated to the alternative site or how the software would be made available at this site to process data. The lack of this information in the plan could impair the Geological Survey's ability to quickly restore this mission-critical system in the event of an emergency. Additionally, the Geological Survey has no assurance that it will be able to continue operations at the alternative site because the contingency plan has not been tested.

Further, SEDAS' computer security plan for 1991, which serves as a management reporting mechanism for providing an overview of the system's security measures, did not accurately describe the status of contingency planning. The security plan, which is required by the Computer Security Act, indicated that a contingency plan was in place and operational and judged to be effective. We believe the contingency plan was not effective because it did not address the communications and software issues discussed above and had not been tested. As a result, agency management does not have the accurate information that it needs to make decisions concerning the allocation of security resources to ensure adequate system security. Geological Survey officials responsible for the system agreed with this assessment. They plan to take corrective action, including updating SEDAS' contingency plan to address the communications and software issues discussed above and developing guidance for testing contingency plans (see enclosures II and III).

- - - - -

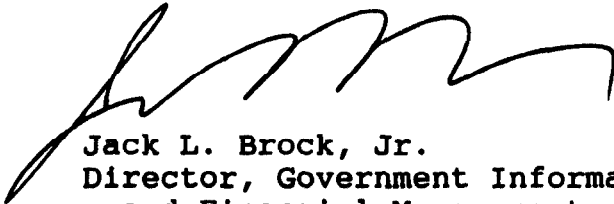
We conducted our review between June 1992 and November 1992, in accordance with generally accepted government auditing standards. We discussed a draft of this letter with appropriate Geological Survey officials, including the Bureau Information Resources Security Administrator

B-251454

and the System Administrator for SEDAS. These officials agreed with our findings and we have incorporated their comments as appropriate.

We are sending copies of this letter to the Chief Geologist, Geologic Division; and the Chief, Office of Earthquakes, Volcanoes and Engineering. Copies will also be made available to others upon request. Should you have any questions about this letter or require additional information, please contact me at (202) 512-6406. Other major contributors to this letter are Linda D. Koontz, Assistant Director; Judith L. Bramlage, Technical Assistant Director; and William J. Dunahay, Senior Evaluator.

Sincerely yours,

A handwritten signature in black ink, appearing to read "J. Brock, Jr.", with a stylized, cursive flourish extending to the right.

Jack L. Brock, Jr.  
Director, Government Information  
and Financial Management

Enclosures (7)

Objective, Scope, and Methodology

Our objective was to test the use of an automated auditing software package, Expert Auditor, to assess technical and operational security controls of a federal system. In cooperation with the Geological Survey, we used Expert Auditor to review the safeguards, techniques, and controls in place to protect SEDAS, the data analysis module of the National Earthquake Information System, and associated computer resources.

We interviewed Geological Survey personnel responsible for computer security at the Geological Survey headquarters and personnel responsible for the operation, administration, and security of SEDAS at the National Earthquake Information Center in Golden, Colorado. We also visited the Center to evaluate computer security practices.

We examined SEDAS' 1990 and 1991 computer security plans, the risk profile report on SEDAS, and other relevant records. We accessed SEDAS information to evaluate the use of audit trails, identification and authentication techniques, and system privileges.

We performed our work at the National Earthquake Information Center, in the Colorado School of Mines, in Golden, Colorado; and at the Geological Survey headquarters in Reston, Virginia.

Contingency Planning

Office of Management and Budget (OMB) Circular A-130 requires agencies to maintain disaster recovery and continuity of operations plans for all information technology installations to provide reasonable continuity of data processing support should events prevent normal operations. In addition, the Geological Survey's manual requires each computer facility to have a plan to ensure automated data processing support to users during interruptions, emergencies, and disasters.<sup>1</sup> This plan is expected to be reviewed annually to determine whether the practices associated with retention and storage of backup files, programs, and documentation are current, complete, and readily usable as intended.

Although the Geological Survey has developed a contingency plan for SEDAS, this plan is incomplete. The existing contingency plan for SEDAS identifies the Geological Survey's computer center in Denver, Colorado, as the alternative site, but does not address how the seismic data, currently communicated to SEDAS via satellite and INTERNET, would be communicated to the alternative site.

In addition, the alternate site does not have a copy of the Seismic Data Analysis System software and access to the backup copy, which is maintained at the current off-site location in Golden, Colorado, would not be timely. Moreover, the off-site backup copy may be at risk depending on the severity of the disaster because it is located in the same general geographical area as the original. In our opinion, the lack of such information in the plan would impair the Geological Survey's ability to quickly restore this mission-critical system in the event of an emergency.

OMB Circular A-130 also requires agencies' continuity of operations plans, for large systems and systems that support essential agency functions, to be fully documented and operationally tested periodically, at a frequency commensurate with the risk and magnitude of loss that could result from disruption of information technology support. As of November 1992, SEDAS' contingency plan had not been tested. Unless the plan is tested periodically, there is no assurance that the Geological Survey would be able to recover from a disaster and provide information technology support for essential agency functions.

---

<sup>1</sup> Geological Survey Manual, Information Systems Security and Control, 500.16.1, October 1982.

Management Reporting

The Computer Security Act of 1987 and OMB Bulletin 90-08 require agencies to develop computer security plans for sensitive automated information systems. These plans serve as a management reporting mechanism for providing an overview of the system's security measures.

SEDAS' 1991 computer security plan inaccurately described that a contingency plan was in place and operational, and judged to be effective. We believe the contingency plan was not effective because it did not address certain communications and software issues and it had not been tested. As a result, agency management does not have accurate information for making decisions concerning the allocation of security resources to ensure adequate system security.

Privacy Data

The Privacy Act requires federal agencies to provide adequate safeguards to ensure information security and confidentiality. SEDAS was not designed to protect against the disclosure of privacy data because the Geological Survey did not intend to use the system to process privacy data. During our visit to the National Earthquake Information Center, we observed a printer connected to the system printing employee salary projections in an area accessible to all center employees. This type of information is normally considered privacy data and should be protected from disclosure to unauthorized personnel. The system manager was not aware that this type of information was being processed on the system. The system administrator told us the Geological Survey will remove privacy data from SEDAS or will develop appropriate controls and procedures for safeguarding this type of data.

### Training

The Computer Security Act of 1987 requires federal agencies to provide periodic training in computer security awareness and accepted computer security practice to all employees who are involved with the management, use, or operation of federal computer systems. Federal guidance advises agencies to design training for each audience category--executives; program and functional managers; IRM, security, and audit personnel; ADP management, operations, and programming staff; and end users. As an example, executives should receive awareness level training in computer security basics and policy level training in security planning and managing. The guidance suggests that agencies design a training program by selecting those topics that provide employees with the skills at a level appropriate to their current position.

Although end user training has been provided at the Center, limited training in computer security awareness and accepted computer security practices has been provided to employees who manage SEDAS. Although the system manager received end user training, he did not receive the more detailed operational training appropriate for his job. Additionally, the site manager had not been trained in computer security awareness and accepted computer security practices. Training designed to meet the learning objectives of managers involved with the daily management and operations of the system would provide those managers with the skill or ability to design, execute, or evaluate agency computer security procedures and practices. On the other hand, training designed for the executives would include awareness training in computer security issues, policies, procedures, and contingency planning. This training would raise awareness about the threats and vulnerabilities of computer systems and the recognition of the need to protect data, information, and the means of processing them. The security administrator told us that the Geological Survey has a large ongoing, nationwide training program and plans to provide the appropriate level of training to these individuals.



Access Control

The Geological Survey's manual requires that access to computer files containing sensitive information be controlled.<sup>2</sup> A specific individual's right to read, copy, or modify a given file should be clearly defined by the application system owner. At the time of our review, however, the access controls in place on SEDAS did not prevent users from accessing and reading information they had no need to know such as the system's accounting data. Accounting data should be protected to minimize the knowledge a user can obtain about other users because this information could help a user access information and system resources he/she was not authorized to use. We discussed this issue with the system manager and he altered the file privileges to ensure appropriate access controls.

---

<sup>2</sup> Geological Survey Manual, Information Systems Security and Control, 500.16.1, October 1982.

Password Management

The Geological Survey's handbook requires that passwords must be protected from disclosure and changed frequently to prevent unauthorized use of the computer system.<sup>3</sup> The Geological Survey's recommended format is two words separated by a nonalphabetic character. This provides for passwords that are easy to remember and virtually impossible for an unauthorized person to guess.

At our suggestion, the system administrator used a software package to check the adequacy of passwords used on SEDAS and found that 34 of about 130 accounts had passwords that did not conform to the Geological Survey's recommended format. These passwords could be easily guessed and, as a result, could allow an unauthorized user access to the system. For example, some of the passwords were the same as the user's identification and many of the others were words from a dictionary. Three of these accounts had system privileges. All of these users subsequently received notices to change their passwords. The system administrator told us that in about a month he plans to use the software package again to check the adequacy of passwords.

---

<sup>3</sup> U.S. Geological Survey Handbook, Management and Use of Small Computer Systems, 500-16-H, July 1985.