~~24678~~
122958

UNITED STATES GENERAL ACCOUNTING OFFICE
REGIONAL OFFICE
Room 1992, Federal Building
Seattle, Washington 98174

MAR 18 1983

122958

Mr. Peter T. Johnson, Administrator
Bonneville Power Administration
Department of Energy
P. O. Box 3621
Portland, Oregon 97208

Dear Mr. Johnson:

Subject: Bonneville Power Administration Control System's Computer Security--More Needs To Be Done (B-211147).

As part of our recent review of automatic data processing (ADP) management at Bonneville Power Administration (Bonneville), we made a limited review of computer security at the control system's Dittmer computer center in Vancouver, Washington. Although Bonneville has made some strides towards developing and implementing a computer security program, as required in Office of Management and Budget (OMB) Circular A-71, Transmittal Memorandum Number 1 [1]/ and Department of Energy (DOE) Order 1360.2, [2]/ it needs to do more.

Recently Bonneville's Division of System Operations appointed a computer protection program manager (CPPM), identified critical and sensitive data processing systems, and assessed risks and threats to the Dittmer computer center's on-going operations. However, during our review we found that:

--Written computer security procedures for the Dittmer computer center have not been developed or implemented. The CPPM said that he was drafting procedures, but would not finalize them until he ensured their compatibility with Bonneville's general-purpose computer security

---

1/Office of Management and Budget Circular A-71 Transmittal Memorandum Number 1, "Security of Federal Automated Information Systems," July 27, 1978.

2/Department of Energy Order 1360.2, "Computer Security Program For Unclassified Computer Systems," March 9, 1979.

122958
525037

procedures which had not yet been completed. We believe the lack of written computer security procedures provides the potential for actions or activiities to take place that could lead to data processing system or computer hardware misuse, abuse or loss.

--An automatic fire suppression system in the Dittmer computer center has not been installed. Ever since 1977 Bonneville had discussed whether it should install an automatic fire suppression system in the Dittmer computer center, and if so what type it should install. Although potential for a major fire is remote, the September 1982 risk assessment estimated that damages could range from $20,000 to $4.1 million for the loss of one data processing system or about $24 million for the loss of the entire Dittmer computer center. In November 1982, 5 years after Bonneville began to discuss the need for an automatic fire suppression system, an Office of Engineering and Construction engineer responsible for the design of the automatic fire suppression system stated he was preparing the final drawings for the computer center's automatic fire suppression system. If approved, the automatic suppression system is scheduled for installation by June 1983.

--Physical access to the Dittmer computer center has not been appropriately restricted. Physical access to the control system's computer center is by card key, and combination lock. In September 1982, 112 persons from the Division of System Operations had access to the Dittmer Building's basement area where the computer center is located. These personnel included the Director, secretaries, clerk-typists, electrical engineers, control systems monitors, systems dispatchers, and computer specialists. In addition, 159 persons from outside the Division of System Operations had access to the building's basement area. Furthermore, in September 1982 the completed risk assessment reported that the combination locks for the computer operations area had not been changed for at least a year, and nearly everyone in the Dittmer Building knew the combination. In January 1983, the CPPM confirmed that the combination of the computer center door locks were still unchanged. In our opinion, access to a computer operations area containing more than $10 million of computer hardware should be limited to only persons who routinely work in the computer operations area. This restriction minimizes the opportunity for tampering, misuse, theft, and vandalism to the computer hardware and data processing systems. Others using the computer operations area infrequently should be escorted.

--A contingency plan for the Dittmer computer has not been fully developed. In November 1982 the CPPM said that he was drafting contingency plan procedures. The September 1982 risk analysis noted that if one of the primary computer processors became nonoperational, most of the data processing systems had a second computer processor available to ensure that control system's operations could continue. However, because primary and backup computer processors sit side by side a major disaster (such as fire, earthquake, or flood) at the computer center could render the data processing system's dual computer processors nonoperational. If both computer processors were inoperable, Bonneville would have to operate the data systems manually. Revenues lost to Bonneville because of manual operation for just 3 days can range from just a few dollars to $150,000, depending on the system that was not operating. According to the CPPM, Bonneville will evaluate the feasability of making the control system's Eastern control computer center at Moses Lake, Washington the off-site computer backup location for the major data processing systems.

Bonneville will have to correct these conditions at the Dittmer computer center before it can fully install a computer security program. To ensure that progress continues, we recommend that you:

--Develop a time phased action plan and feedback procedures to (1) complete the Dittmer computer center security procedures; (2) install a fire suppression system at the computer center; (3) evaluate Division of System Operations policies and procedures regarding physical access to the computer center; and (4) complete, implement, and test the computer center's contingency plan.

--After the computer security program is implemented, direct the chief auditor to periodically review the computer centers security program's implementation and its compliance with OMB Circular A-71 Transmittal Memorandum Number 1 and DOE Order 1360.2.

We are sending copies of this report to the Director, Office of Management and Budget; and the Secretary of Energy. We appreciate the courtesies and cooperation extended to our representatives during our review.

Sincerely yours,

Walter H. Henson
Regional Manager