124360
~~28467~~

UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

RESOURCES, COMMUNITY
AND ECONOMIC DEVELOPMENT
DIVISION

May 24, 1984

124360

Mr. William Bettenberg
Director, Minerals Management Service
Department of the Interior

Dear Mr. Bettenberg:

Subject: Safeguarding of Proprietary Data at Minerals Management Service OCS Regional Offices (Code 005578)

As part of our ongoing assignment entitled "Review of the Department of the Interior's Ability to Access and Use Outer Continental Shelf (OCS) Data," we reviewed Minerals Management Service's (MMS) procedures for assuring the confidentiality of proprietary data. Data are considered proprietary when, if disclosed, they could result in significant competitive disadvantage and financial loss to the owner. Proprietary data are frequently furnished by private companies to MMS in the conduct of the offshore oil and gas leasing program. For example, proprietary geological and geophysical data used by companies to identify potential oil and gas resources are furnished to MMS.

This letter is to apprise you of instances we found where MMS regional offices are not complying with Interior or government-wide standards for safeguarding proprietary data, and of the need for appropriate corrective action. These observations are being provided to you at this time because we recognize that MMS is attempting to improve its safeguarding of proprietary data and believe that these observations will be helpful in this effort.

At the four OCS regional offices, we reviewed the results of physical security and computer-related inspections done by MMS headquarters' security officers, interviewed regional security officials, and observed regional office physical and automated data processing (ADP) security measures. As part of our review, regional security officials completed a physical security checklist--the same checklist used by MMS inspectors. Our field work was conducted between October 1983 and March 1984.

We reviewed two aspects of safeguarding: the physical security of the regional offices and the controls over ADP systems within the regional offices. We also determined whether MMS conducted risk analyses to identify the appropriate level of security. MMS is required by the OCS Lands Act, the Financial Integrity Act, and by its own policies to protect proprietary data in its possession. MMS' standards for protecting proprietary data are specified in United States Geological Survey Instructional Memorandum Number 78-05-RE as approved on April 27, 1979. We used these standards as a basis for our interviews and observations about physical security. We used the government-wide computer security standards, "Federal Information Processing Standards Publication 31 "Guidelines for Automatic Data Processing, Physical Security, and Risk Management" (U.S. Department of Commerce, National Bureau of Standards, June 1974) and Interior's Departmental Manual to evaluate MMS' ADP facilities. We conducted our review in accordance with generally accepted government auditing standards.

We found that many of Interior's requirements for physically safeguarding proprietary data in the OCS regional offices are not being met and that there is also inadequate control over ADP operations which use proprietary data. Further, risk analyses had not been conducted to determine the appropriate level of security for proprietary data used by MMS.

IMPORTANCE OF SAFEGUARDING PROPRIETARY DATA

Although we did not find instances where proprietary data held by MMS' OCS regional offices had been improperly disclosed, industry representatives have been concerned about MMS' ability to safeguard potentially highly valuable proprietary data provided by companies. This concern has increased with recent changes to MMS' presale planning process whereby MMS plans to gain greater access to industry planning and exploration data, depending on the circumstances of the sale. At the American Petroleum Institute OCS Panel Meeting in February of this year, industry representatives expressed concern about how much confidential exploration data, some of which may involve interpretive data, should be given to MMS during its planning process.

Interior's Inspector General's Office is conducting its own assessment of MMS' ADP security procedures for proprietary data and plans to issue its draft report about mid-June. MMS security officials have also inspected or plan to inspect all OCS regional offices during 1983-84. Prior MMS inspections disclosed many of the same security deficiencies which we found. Also, MMS headquarters officials are also developing a new chapter to the departmental manual which outlines the policies, responsibilities, and procedures for safeguarding proprietary data. MMS expects to issue this chapter within the next 2 months. In addition, MMS officials said the Alaska OCS regional office will be consolidated in a new building later this year and this should provide better security arrangements for proprietary data.

PHYSICAL SECURITY MEASURES NEED IMPROVEMENT

We found that many of Interior's requirements for the physical safeguarding of proprietary data are not being met. In the four OCS regional offices, we found 19 instances where access by unauthorized persons is not adequately controlled or where physical protection of storage areas does not meet Interior's standards. For example, we found that three OCS regional offices do not require employees to wear identification badges. Although it is not a requirement that employees wear identification badges, the Interior manual and MMS security office suggest that badges be worn by employees to help ensure that only properly authorized persons are allowed in work areas. The Gulf of Mexico regional office is the only region which has this requirement although the Atlantic regional office is considering such a requirement.

In addition, we found that the regional offices need to install and use proper locking devices in work areas. We found that only the Atlantic OCS regional office had proper deadbolt locks on all work areas.

Enclosure I summarizes the results of our evaluation of the regional offices' physical security, based on Interior's standards.

ADP SECURITY NEEDS STRENGTHENING

Based on our inspections, we found that all four OCS regional offices have inadequate internal controls in their ADP operations which use proprietary data. We inspected 16 computer security items at each OCS regional office and found 40 instances where the offices did not comply with government-wide computer security standards.

We found that OCS regional offices needed to:

--establish proper procedures for backing up computerized data. For example, Interior's manual requires that critical original and backup ADP files be physically separated by one mile; however, none of the regions are complying with this requirement.

--establish proper controls over access to the system. Although Interior's manual requires that critical ADP functions be separated so that no person is able to control all parts of the system, only the Gulf of Mexico OCS regional office maintains this separation of power.

--identify computer tapes and output with the "proprietary" label. The Gulf of Mexico OCS regional office is the only office which automatically places a label on both tapes and outputs.

--protect computer equipment which can be accessed by telephone, since such systems are vulnerable to unauthorized intrusion. However, regional offices use only password security procedures to prevent unauthorized intrusion.

Enclosure II summarizes our findings at the OCS regional offices.

RISK ANALYSES HAVE NOT BEEN PERFORMED

The four OCS regional offices have not completed risk analyses to determine the appropriate level of security needed for proprietary data. The Federal Manager's Financial Integrity Act of 1982 (Public Law 97-255) mandated renewed focus on the need for federal agencies to strengthen internal controls. The Standards for Internal Controls in Federal Government (U.S. General Accounting Office, 1983) were established in response to this mandate. The internal control standards specify that agencies are to identify:

--risks inherent in agency operations;

--criteria for determining low, medium, and high risks; and

--acceptable levels of risk under varying circumstances.

In addition, Interior's manual requires that a risk analysis be done for each computer installation at least once every 5 years in order to:

--quantify assets which require protection;

--establish the sensitivity of ADP system applications;

--analyze threats to determine possible adverse impacts on the system and installation (threats to be analyzed include natural hazards, accidents, and intentional acts);

--specify the probability of an occurrence;

--determine the exposure of ADP systems to loss for a given time period; and

--identify safeguards which should be implemented.

However, risk analyses had not been conducted at any of the OCS regional offices.

- - - -

We have kept Interior Inspector's General's staff informed as this assignment progressed. Because of the Inspector General's ongoing effort and interest in data security, we will forward a copy of this letter to that office. We are also available to discuss our detailed observations regarding the security of proprietary data with MMS officials and the Interior Inspector General's staff.

Because this assignment is part of a request received from the Chairman, Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce, he will be provided a copy of this letter. We plan to make no further distribution of this letter.

We thank you for the cooperation and courtesies which you and your staff have extended to us.

Sincerely yours,

F. Kevin Boland

F. Kevin Boland
Senior Associate Director

Results of GAO's Physcial Security Inspections at OCS Regional Offices[a]

Security concern	Alaska	Atlantic	Gulf	Pacific
Are procedures implemented for assuring that visitors are authorized and controlled?				
—Are visitor badges numbered and controlled?	No	No	Yes	Yes
—Do all entrances have visitor controls?	No	No	No	No
Is the distribution of keys to employees restricted?	No	No	Yes	Yes
Do employees wear identification badges?	No	No	Yes	No
Are construction criteria for storage areas met?	No	Yes	Partial	No
Are intrusion alarms present in areas where proprietary data is stored?	Yes	Yes	No	Yes
Are windows obscured to prevent visual access to proprietary data being used in work areas?	No	No	No	Yes
Are key-operated deadbolt locks or other secure locking systems used for work area doors?	Partial	Yes	Yes	Partial
Is proprietary data safeguarded when custodians are in work areas?	Yes	Yes	Yes	Yes
Is proprietary data returned to an appropriate storage area at night?	Yes	Yes	No	Yes
Are alarms monitored after hours?	Yes	Yes	No	Yes

[a] Based on U.S. Geological Survey Instructional Memorandum Number 78-05-RE.

Results of GAO's Computer Security Inspections at OCS Regional Offices[a]

Security concern	Alaska	Atlantic	Gulf	Pacific
Has a risk analysis been performed to determine sensitivity of the ADP system to threats and identify proper safeguards?	No	No	No	No
Does the facility have a tape library or filing system which controls the checkout, check-in, and location of tapes?	No	No	No	No
Is proprietary data labeled as such on both tapes and outputs?	No	No	Yes	No
Does the facility follow Interior's Departmental Manual requirements for authorizing access to the system? For example, are critical functions separated--does one person, need authorization from a second person in order to run equipment, access, and make changes to data?	No	No	Yes	No
Is computer equipment protected from unauthorized access by telephone?	Yes	Yes	No	Yes
Does the facility adhere to Interior's Departmental Manual requirements for the storage of data and software?				
--are data and software backed up?[b]	Yes	Yes	Yes	Yes
--are backups separated from originals?	No	No	No	No
Is access to the computer facility restricted?	No	Yes	Yes	Yes
Do employees wear identification badges?	No	No	Yes	No
Do computer room doors have proper locks?	No	Yes	Yes	Yes
Are computer facilities protected by intrusion alarms?	No	No	No	No
Are computer facilities protected by fire alarms?	Yes	Yes	No	No
Does the facility have proper fire extinguishing equipment immediately available?	No	Yes[c]	Yes	Yes
Does the facility have contingency or emergency plans to provide for continued operation under abnormal conditions?	No	No	Yes	No
Are ADP facilities clean and orderly?	No	Yes	No	No
Are cleaning crews monitored by MMS staff while in the ADP facility?	No	Yes	No	No

[a] Based on Federal Information Processing Standards Publication 31.

[b] The time interval for backing up data varied from weekly in the Pacific OCS region to once every 2 to 3 months in the Alaska OCS region.

[c] This is a water sprinkler system which could endanger equipment and lives, if discharged.