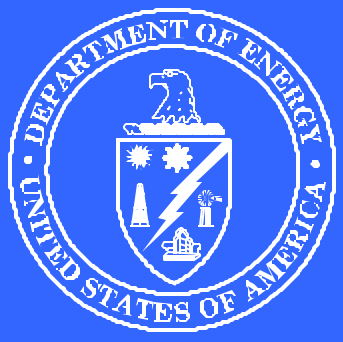
DOE/IG-0531

INSPECTION REPORT



U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL
OFFICE OF INSPECTIONS

INSPECTION OF CYBER SECURITY STANDARDS FOR SENSITIVE PERSONAL INFORMATION

NOVEMBER 2001

U.S. DEPARTMENT OF ENERGY
Washington, DC 20585

November 13, 2001

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman /s/
Inspector General

SUBJECT: INFORMATION: Report on "Inspection of Cyber Security Standards for Sensitive Personal Information"

BACKGROUND

The Office of Inspector General (OIG), U.S. Department of Energy (DOE), identified a concern relating to the cyber security of unclassified sensitive personal information maintained by the Department under the Privacy Act of 1974, and other personal information exempt from disclosure under the Freedom of Information Act (Privacy Act/FOIA personal information). Specifically, the concern related to possible compromise of this type of information on or over DOE Headquarters and field site computer networks.

RESULTS OF INSPECTION

The OIG concluded that the Department does not always meet the requirements of the Privacy Act of 1974, the Freedom of Information Act, or the Computer Security Act of 1987 because the Department: 1) does not have a Department-wide baseline criteria for protecting Privacy Act/FOIA personal information; 2) does not group Privacy Act/FOIA personal information with other unclassified sensitive information for protection; and 3) allows individual sites and program offices to develop differing security measures for protection of Privacy Act/FOIA personal information.

We recommended that the Administrator, National Nuclear Security Administration and the Chief Information Officer, in conjunction with the Director, Freedom of Information and Privacy Acts Division evaluate the need for additional policy or direction regarding Department-wide security requirements to protect Privacy Act/FOIA personal information maintained on, or transmitted to and from, Department computer systems connected to the Internet, Intranet (e.g., DOEnet), or e-mail.

MANAGEMENT REACTION

The OIG received two sets of comments. One set was from the Director, Freedom of Information and Privacy Acts Division, and the second set represented the combined comments of the Acting Chief Information Officer (Acting CIO) and the Associate Administrator for Management and Administration, National Nuclear Security Administration. Management concurred with the recommendation.

The Director, Freedom of Information and Privacy Acts Division, stated that several actions will be initiated to protect Privacy Act/FOIA personal information. These actions include action by the Office of Management, Budget and Evaluation, (formerly the Office of Management and Administration), and the Chief Financial Officer, to install a Secure Socket Layer, which provides additional protection and confidentiality, for all servers maintaining personal information under their purview.

The Acting CIO and Associate Administrator for Management and Administration disagreed that Department-wide baseline criteria was necessary for all DOE elements in order to protect Privacy Act/FOIA personal information. However, they stated that the need for policy in this area will be a topic of discussion at the next Cyber Security Policy Working Group (PWG) meeting scheduled for October 2001.

The PWG meeting was held on October 24, 2001. One topic of discussion at the meeting was the development of a "Departmental Unclassified Cyber Security Management Program Manual." The manual's objectives are to establish requirements for the unclassified cyber security program, including the protection of all the Department's information resources. A draft of the manual will be discussed further at the next PWG meeting which is scheduled for January 2002. The manual is expected to be completed in June 2002. We are hopeful that the manual will include minimum cyber security measures for protecting Privacy Act/FOIA personal information.

Attachment

cc: Deputy Secretary
Administrator, National Nuclear Security Administration
Acting Chief Information Officer
Director, Freedom of Information and Privacy Acts Division
Director, Office of Management, Budget and Evaluation
Director, Office of Executive Secretariat

INSPECTION OF CYBER SECURITY STANDARDS FOR SENSITIVE PERSONAL INFORMATION

TABLE OF CONTENTS

Overview

INTRODUCTION AND OBJECTIVE

The Office of Inspector General, U.S. Department of Energy (DOE) identified a concern relating to the cyber security of unclassified sensitive personal information. This includes information within systems of records maintained by the Department under the Privacy Act of 1974 (Privacy Act), and other personal privacy-type information that may be exempt from disclosure under the Freedom of Information Act (FOIA). Specifically, the concern related to possible compromise of this type of information on or over DOE Headquarters and field site computer networks.

The Department currently has 38 field sites networked by intranet via the Department's corporate computer network entitled "DOEnet" (see Appendix B). DOEnet "is a centrally managed, closed network, operated over Sprint's public communications paths, designed to carry business sensitive data to users throughout the DOE federal sites." There are several DOE systems, referred to as applications, that use DOEnet or are accessed through the DOEnet. Examples include: the Corporate Human Resource Information System (CHRIS); Energy Time and Attendance; the DOEInfo database system; the Primary Organizational Web-Based Employee Records; and Travel Manager, which interfaces with the Departmental Integrated Standardized Core Accounting System. A complete listing of DOEnet applications, not all of which contain personal information, is at Appendix C.

One DOE system, the DOEInfo database system, is a repository of substantial information relating to the DOE Federal workforce. This database contains unclassified sensitive personal information that may be subject to the Privacy Act and other personal information that may be exempt from disclosure under the FOIA (to be referred to as Privacy Act/FOIA personal information). This information includes employee personal information; payroll; salary and benefits; manpower (FTE) data; Social Security numbers; and employee locator information.

There are three ways to access the DOEInfo database: through the Internet, through the DOEnet intranet, or by a hardwire to the mainframe computer. DOEInfo is encrypted if it is accessed via the Internet. However, DOEInfo is unencrypted as it is housed on its server connected to DOEnet and is unencrypted when accessed via the DOEnet. This is because DOEnet is often considered to be a private network although it is operated over the Sprint network. Additionally, e-mail that is routed daily throughout the Department may contain Privacy Act/FOIA personal information. Unencrypted e-mails sent over the DOEnet are not secure.

The objective of this inspection, therefore, was to determine whether the Department's cyber security program meets the requirements of the Privacy Act of 1974, the Freedom of Information Act, and the Computer Security Act of 1987, to adequately protect Department employees' Privacy Act/FOIA personal information from the risks associated with unauthorized disclosure.

CONCLUSION AND OBSERVATIONS

We concluded that the Department does not always meet the requirements prohibiting unauthorized disclosure of Privacy Act/FOIA personal information addressed in the Privacy Act of 1974, the Freedom of Information Act, and the Computer Security Act of 1987. The Department: 1) does not have Department-wide baseline criteria for protecting Privacy Act/FOIA personal information; 2) does not group Privacy Act/FOIA personal information with other unclassified sensitive information for protection; and 3) allows individual sites and program offices to develop differing security measures for protection of Privacy Act/FOIA personal information. The Privacy Act of 1974 provides controls on maintenance of information in a Privacy Act system of records, the Freedom of Information Act provides exemptions from disclosure, and the Computer Security Act provides that this type of data be treated, and protected, in the same manner as national interest information.

Guidelines for the Privacy Act/FOIA personal information for the Department is managed by two offices - the Freedom of Information Act/Privacy Act Office, under the purview of the Office of Management and Administration; and the Office of the Chief Information Officer (CIO), under the purview of the Office of Security and Emergency Operations.[1] Although the CIO recently purchased 20,000 Public Key Infrastructure (PKI) licenses with encryption capability, there is no DOE requirement that the PKI be used as a security measure for e-mail and file data transfers by DOE employees. At present, the Department, which includes the National Nuclear Security Administration, does not have Department-wide uniform controls, such as encryption, to protect Privacy Act/FOIA personal information. As a result, the Department has no baseline cyber security requirement to ensure adequate security of Privacy Act/FOIA personal information. Instead, the Department's current policy allows each DOE site to determine the risk associated with the loss of Privacy Act/FOIA personal information when implementing cyber security. Each

[1] Effective October 1, 2001, the Offices of Management and Administration and the Chief Financial Officer were merged and renamed the Office of Management, Budget and Evaluation. Additionally, the Chief Information Officer became a separate office reporting to the Office of the Secretary.

DOE site, therefore, may have differing security measures for Privacy Act/FOIA personal information though that type of information is the same throughout the Department.[2]

From a security standpoint, each site prepares against what the site determines to be a security threat. That site may not determine that the risk for loss of Privacy Act/FOIA personal information to be as high a security threat as another site, but threats to Privacy Act/FOIA personal information is not site-specific. The risk to Privacy Act/FOIA personal information is the same throughout the Department as long as it is on the DOEnet.

We concluded there should be a baseline policy throughout the Department concerning the protection of Privacy Act/FOIA personal information to protect DOE employees and guard against the risk of compromise of their personal information. These risks include identity theft and intelligence targeting; and the risk of potential litigation against the Department if the Department is remiss in its responsibility to protect Privacy Act/FOIA personal information.

[2] The focus of this review was on Department-wide policy and, therefore, this inspection did not evaluate the cyber security measures taken at individual sites.

Details of Findings

Cyber Space Protection for Unclassified Sensitive Information

DOE Notice DOE N 205.1, "Unclassified Cyber Security Program,"[3] initiated by the Office of the Chief Information Officer, establishes the framework for the Department's Unclassified Cyber Security Program.

DOE N 205.1 directs each Departmental organization to develop an individual Cyber Security Program Plan for protecting DOE information and information systems. The Cyber Security Plan is based on an organization's risk assessment of its environment, mission, and possible threats weighed against the harm incurred if information is lost, misused, disclosed, or modified without authorization. An objective of DOE N 205.1 is "To ensure that the DOE Unclassified Cyber Security Program achieves the objectives of Federal and State regulations, Executive Orders, national security directives, and other regulations."

DOE N 205.1 states that Privacy Act/FOIA personal information, along with Unclassified Controlled Nuclear Information, Naval Nuclear Propulsion Information, and Export Controlled Information, may require additional performance measures when a DOE site or program office develops its Cyber Security Program Plan. According to an official from the Office of the Chief Information Officer, DOE N 205.1 identifies two categories of unclassified sensitive information. In the first category, the Department "owners" of Unclassified Controlled Nuclear Information, Export Controlled Information, and Naval Nuclear Propulsion Information, have provided policy on how these types of unclassified sensitive information are to be managed throughout the Department. Therefore, when a DOE site or program office is developing its specific Cyber Security Program Plan, that site or program office must include the security requirements of Federal and state regulations, Executive Orders, national security directives, and also Department "owner" regulations. For example, the Department "owner" of Unclassified Controlled Nuclear Information requires encryption if the information is being transmitted over a public communications path.

The second category identified in DOE N 205.1, includes Privacy Act unclassified sensitive information. The Notice does not require a Department-wide standard for all sites when protecting Privacy Act/FOIA personal information. Each DOE element can tailor its own protection mechanisms.

[3] The CIO has recently issued for comment Draft DOE O 205.1, "Departmental Cyber Security Management Program." The Draft Order does not provide any additional security measures specific to Privacy Act/FOIA.

The DOEnet and E-mail

In addition to the concern that site-specific Cyber Security Program Plans may not be adequately protecting Privacy Act/FOIA personal information, there is a risk of compromise for Privacy Act/FOIA personal information accessible via DOEnet applications and used in e-mails. DOEnet is a private network run on a public communications path. DOEnet officials told us that the application owner is responsible for applying appropriate security measures. Several application owners include Privacy Act/FOIA personal information in the data connected to or transmitted over DOEnet. Some application owners have applied encryption to the data when it is accessed via the Internet, but other owners have not.

DOE employee e-mails sometimes contain personal information that may be subject to the Privacy Act/FOIA. According to a Headquarters information technology official, if e-mails are not encrypted then it is "buyer beware." In other words, the intended recipient may not be the only individual receiving the e-mail. According to a May 11, 2000, memorandum, from the then CIO, "All should be aware that information sent over the Internet or as attachments to electronic mail can be monitored, recorded, and accessed by the general public."

Department Privacy Act/FOIA Personal Information Oversight

There are two "owners" providing policy on Privacy Act/FOIA personal information. "Owners" are the system managers, or custodians, of data for the Department's system of records. The first "owner" is the Freedom of Information Act/Privacy Act Office, Office of the Executive Secretariat, Office of Management and Administration, which is responsible for administering policies, programs, and procedures for management of Privacy Act/FOIA personal information throughout the Department. However, under the Office of Management and Budget Circular A-130, "Management of Federal Information Resources," the second "owner" is the Office of the Chief Information Officer, Office of Security and Emergency Operations, which is assigned authority over Privacy Act/FOIA personal information.

We determined that the "owners" have not provided adequate protection requirements throughout the Department because the Freedom of Information Act/Privacy Act Office and the Office of the Chief Information Officer have not required a baseline Department-wide standard for all sites. A baseline standard would assist the Department in protecting its Privacy Act System of Records from unauthorized disclosure and protection in the same manner as national interest information.

The Computer Security Act, The Privacy Act, and FOIA

As indicated above, DOE N 205.1 treats Privacy Act unclassified sensitive information (Privacy Act/FOIA personal information) differently than Unclassified Controlled Nuclear Information, Naval Nuclear Propulsion Information, and Export Controlled Information. We determined that this may be inconsistent with the intent of the Computer Security Act of 1987 (Public Law 100-235), which treats Privacy Act information in the same way as national interest information, such as Unclassified Controlled Nuclear Information, Naval Nuclear Propulsion Information, and Export Controlled Information. Specifically, the Computer Security Act of 1987 defines sensitive information to include any information that "the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act)." In addition, for information maintained in a system of records, the Department is required by the Privacy Act to:

> . . . establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

Also, according to FOIA, information exempted from disclosure contains "personnel . . . and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."

Appendix III to Office of Management and Budget (OMB) Circular No. A-130, "Security of Federal Automated Information Resources," establishes minimum controls to be included in Federal automated information security programs and incorporates requirements of the Computer Security Act of 1987 and responsibilities assigned in applicable national security directives. Appendix IV to OMB Circular No. A-130, "Analysis of Key Sections," section 3., "Analysis," requires agencies to provide appropriate protection to government information; assess the risks associated with maintenance and use; and meet the requirements of the Privacy Act of 1974 and the Computer Security Act of 1987.

We determined that the Department does not always meet the requirements prohibiting unauthorized disclosure of Privacy

Act/FOIA personal information addressed in the Privacy Act of 1974, the Freedom of Information Act, and the Computer Security Act of 1987. The Department: 1) does not have Department-wide baseline criteria for protecting Privacy Act/FOIA personal information; 2) does not group Privacy Act/FOIA personal information with other unclassified sensitive information for protection; and 3) allows individual sites and program offices to develop differing security measures for protection of Privacy Act/FOIA personal information.

The Department's failure to ensure security and confidentiality of personal information against threats that can be anticipated is contrary to its own DOE N 205.1 which, as previously cited, requires the DOE Unclassified Cyber Security Program to achieve the objectives of Federal law. Additionally, by not meeting the requirements of the Privacy Act of 1974, the Freedom of Information Act, or the Computer Security Act of 1987: 1) there is the potential for litigation against the Department due to inadequate cyber security; and 2) there is the risk that the Department's employees may be subject to identity theft and intelligence targeting.

The benefit of a baseline cyber security requirement is not only for the individual stationed at any site, but for the Department in meeting the requirements of the Privacy Act of 1974, the Freedom of Information Act, and the Computer Security Act of 1987.

Department-wide Impact

A Department-wide policy on protection of PA/FOIA personal information would not only aid the Department in protecting against security threats and liability, but would assist with protecting employees from potential risks. In spite of the Privacy Act of 1974, the Freedom of Information Act, and the Computer Security Act of 1987, the Department has chosen to allow each "Departmental organization" to develop an individual Cyber Security Program Plan for protecting information and information systems at its site. However, it is the Department's responsibility to protect all its employees, not just those at sites with better cyber security measures. Although there are no absolutes in security, having a baseline security policy for Privacy Act/FOIA personal information is one step closer to ensuring that there will be minimum loss, misuse, or unauthorized access to or modification of the privacy to which individuals are entitled under section 552a of title 5.

The following sections highlight the potential risks of identity theft and intelligence targeting through increased cyber security attacks,

and the need for standard security measures throughout the Department.

Department-wide Cyber Security Risks/Threats

The Computer Incident Advisory Capability (CIAC), an element of the Computer Security Technology Center at Lawrence Livermore National Laboratory was established in 1989 to serve the DOE community. CIAC is recognized nationally and internationally and is a founding member of the "Forum of Incident Response and Security Teams," a "global organization established to foster cooperation and coordination among computer security teams worldwide." The CIAC provides statistical data on the number of cyber security incidents throughout the DOE community. CIAC's Fiscal Year (FY) 1999 Annual Report to the Department identified that "The number of incidents reported to CIAC for FY 1999 increased to 231% of that of FY 1998." The report attributes these incidents to several factors including an "Increased population of potential hackers because of the growth of the Internet," and "The continuing rise in reconnaissance activities [by adversaries] including scans and probes."

CIAC defines a security incident on a computer system as "any adverse event in a computer system or network that threatens the security of the system or network, its data, or availability." Incidents include "scanning, denial-of-service, attempted compromises, or actual compromises called intrusions."

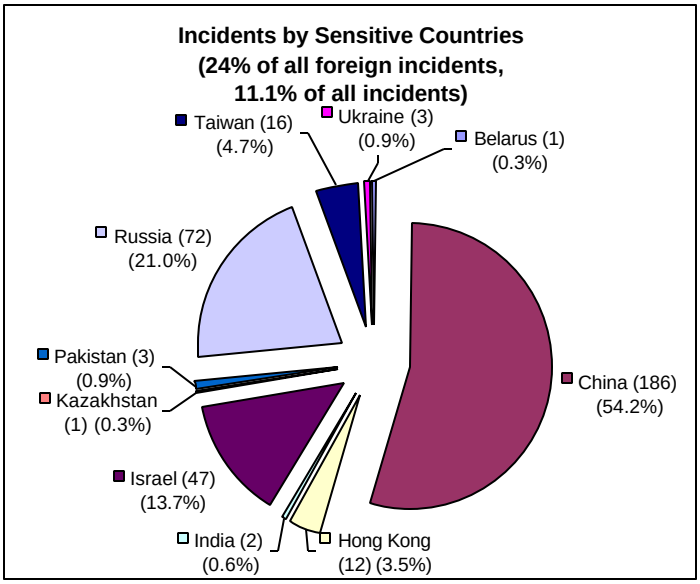
Using a baseline of 103 DOE sites for their report, CIAC handled 3,080 DOE incidents in FY 1999, compared to 1,335 for FY 1998. According to CIAC, there were 130 successful intrusions in FY 1999 as compared to 123 in FY 1998. Forty-six DOE sites reported at least one incident in FY 1999. There may be both counterintelligence and criminal concerns associated with access to Privacy Act/FOIA personal information. As discussed in a recent OIG audit report, "Virus Protection Strategies and Computer Incident Reporting," DOE/OIG-0500, April 2001, the statistics presented above are based on a reporting rate of less than 50 percent.

Counterintelligence Concerns

According to the Department's Nonproliferation and National Security Institute's "Counterintelligence Awareness Guide," "Foreign intelligence collectors are pursuing a broader range of targets, and it is relatively easy for them to establish contact with and assess Americans who have access to valuable classified, controlled or proprietary information." Foreign intelligence operatives can target individuals for contact more easily if they know personal information such as an individual's social security

number, birth date, home address, title, security clearance level, or banking information.

Counterintelligence issues are addressed in DOE O 5670.3, "Counterintelligence Program," which emphasizes the importance of protecting sensitive and proprietary data from foreign nationals and sensitive countries. Counterintelligence concerns are raised by scans and attacks from DOE sensitive countries. This is illustrated for FY 1999 in the following chart.



According to CIAC, of the 3,080 incidents, 1,412 incidents had at least one foreign source. "In looking at the 1,412 incidents involving apparent non-U.S. sources, 40 resulted in an actual system compromise. All of the rest fall into the category of attempts and reconnaissance—scans and probes. These incidents document that DOE systems are the targets of hackers and that the compromise of Privacy Act/FOIA personal information cannot be discounted.

In commenting on the statistics in the draft version of this report, management pointed out that for fiscal year 2001, "intrusion and web defacements has dropped by more than half while the number of scans and probes has escalated by a factor of 10."

Criminal Issues

Criminal issues are addressed, in part, by 18 USC § 1030, "Fraud and related activity in connection with computers," and 18 USC § 1028, "Fraud and related activity in connection with identification documents and information," also known as identity theft. According to the U.S. Postal Inspection Service:

> Identity theft involves acquiring key pieces of someone's identifying information, such as name, address, date of birth, social security number and mother's maiden name, in order to impersonate them. This information enables the identity thief to commit numerous forms of fraud which include, but are not limited to, taking over the victim's financial accounts, opening new bank accounts, purchasing automobiles, applying for loans, credit cards and social security benefits, renting apartments, and establishing services with utility and phone companies.

If, through connection or transmission over DOE computer networks, Privacy Act/FOIA personal information relating to specific individuals is compromised due to inconsistent approaches to security, identity theft could take place and result in substantial harm, embarrassment, inconvenience, or unfairness to the affected individual employee, and potential litigation against the Department.

RECOMMENDATION

We recommend that the Administrator, National Nuclear Security Administration, and the Chief Information Officer, in conjunction with the Director, Freedom of Information and Privacy Acts Division:

Evaluate the need for additional policy or direction regarding a Department-wide security requirement to protect Privacy Act/FOIA personal information maintained on, or transmitted to and from, Department computer systems connected to the Internet, Intranet (e.g., DOEnet), or e-mail.

MANAGEMENT REACTION

The OIG received two sets of comments. One set was from the Director, Freedom of Information and Privacy Acts Division, and the second set represented the combined comments of the Acting Chief Information Officer (Acting CIO) and the Associate Administrator for Management and Administration, National Nuclear Security Administration (Associate Administrator). Management concurred with the recommendation.

FOIA/Privacy Act Director's Comments

The Director, Freedom of Information and Privacy Acts Division stated that the following actions will be initiated:

> "1) Instructions will be issued to all Department FOIA Officers and Contacts to consult and coordinate with their information management

personnel to implement safeguards to protect personal information that is maintained, preserved and transmitted electronically from unauthorized access during electronic transmission.

2) Systems of information will be reviewed to identify any other systems at the Department that may contain personal information and that should be protected from unauthorized access during electronic transmission.

3) The Department's Compilation of System of Records Established Under the Privacy Act will be amended to identify the safeguards that have been established to protect personal information that is maintained subject to the Privacy Act from unauthorized access.

4) Public Key Infrastructure Technology will be developed and implemented by the Office of Management [and] Administration (MA) in conjunction with the Office of the Chief Information Officer to safeguard all systems that maintain, preserve and transmit personal information electronically from unauthorized access."

The Director also stated he had been advised by the Office of Management, Budget and Evaluation that they have identified their systems containing personal information and will work with the Office of the Chief Information Officer to install a Secure Socket Layer for all their servers maintaining personal information. The Director went on to explain that a Secure Socket Layer provides additional protection and confidentiality for the personal information maintained on or transmitted from the servers.

Acting CIO's/ Associate Administrator's Comments

The Acting CIO and Associate Administrator stated that the CIO published DOE Guideline 205.1-1, Cyber Security Architecture, on March 8, 2001. The Guideline recommends Department-wide baseline criteria for protecting all information, including personal information subject to the Privacy Act and FOIA. They also stated that the CIO is establishing a framework of objectives, guiding principles, and security activities and functions, applicable to the classified and unclassified environments, to govern consistent implementation of cyber security management and objectives of Federal and State regulations throughout the Department.

Despite these actions, the Acting CIO and Associate Administrator disagreed with our conclusion that the Department does not always meet the requirements of the Privacy Act, FOIA, or the Computer Security Act because the Department: 1) does not have Department-wide baseline criteria for protecting Privacy Act/FOIA personal information; 2) does not group Privacy Act/FOIA personal information with other unclassified sensitive information for protection; and 3) allows individual sites and program offices to develop differing security measures for protection of Privacy Act/FOIA personal information.

The Acting CIO and Associate Administrator determined that recommending a Department-wide baseline criteria for computer system protection is sufficient guidance to system owners and that system owners are expected to protect sensitive data using the Department's recommended guidance. They stated that DOE policy contains an objective to ensure the confidentiality, integrity, availability, and accountability of information; and that information resources must be protected commensurate with the risks and threats of its environment. They also stated that an agency is not restricted from establishing different security measures across program lines.

The Acting CIO and Associate Administrator agreed that the Department does not have Department-wide uniform controls, such as encryption, to protect Privacy Act/FOIA personal information, but noted that the Department does require each site to evaluate the risks and threats to its information taking into consideration the mission of each organization and the environment in which they operate.

Finally, the Acting CIO and Associate Administrator said that at the October 2001 Cyber Security Policy Working Group (PWG) meeting they would discuss the need for additional policy or direction regarding a Department-wide security requirement to protect personal information. The PWG meeting was held on October 24, 2001, and mentioned development of the Departmental Unclassified Cyber Security Management Program Manual. The manual's objectives are to establish requirements for the unclassified cyber security program, including the protection of all the Department's information resources. It is expected the manual will be completed in June 2002. The next PWG meeting is scheduled for January 2002.

INSPECTOR RESPONSE

The comments provided by the Director, Freedom of Information and Privacy Acts Division, were responsive to the recommendation. Regarding comments from the Acting CIO and Associate Administrator, we are encouraged that the Acting CIO is establishing a framework of objectives, guiding principles, and security activities and functions to govern consistent implementation of cyber security management and objectives throughout the Department. We are also encouraged that the Cyber Security Policy Working Group discussed the need for policy at their October 24, 2001, meeting. However, a representative from the Freedom of Information and Privacy Acts Division was not in attendance at the meeting. We recommend that all parties responsible for protection of Privacy Act/FOIA personal information be included in future meetings.

We continue to believe that guidance for Department-wide baseline criteria is inadequate because Departmental guidance does not require all DOE elements to take minimum cyber security measures for protecting Privacy Act/FOIA personal information. We agree with management that open science, on one hand, and national defense, on the other hand, do not need the same level of cyber security. However, the personal information concerning an employee located at the Thomas Jefferson National Accelerator Facility should have the same minimum protection as an employee at the Y-12 National Security Complex. The cyber risk to these employees is the same regardless of their office affiliation or location.

Management's general comments have been incorporated into the report where appropriate.

Appendix A

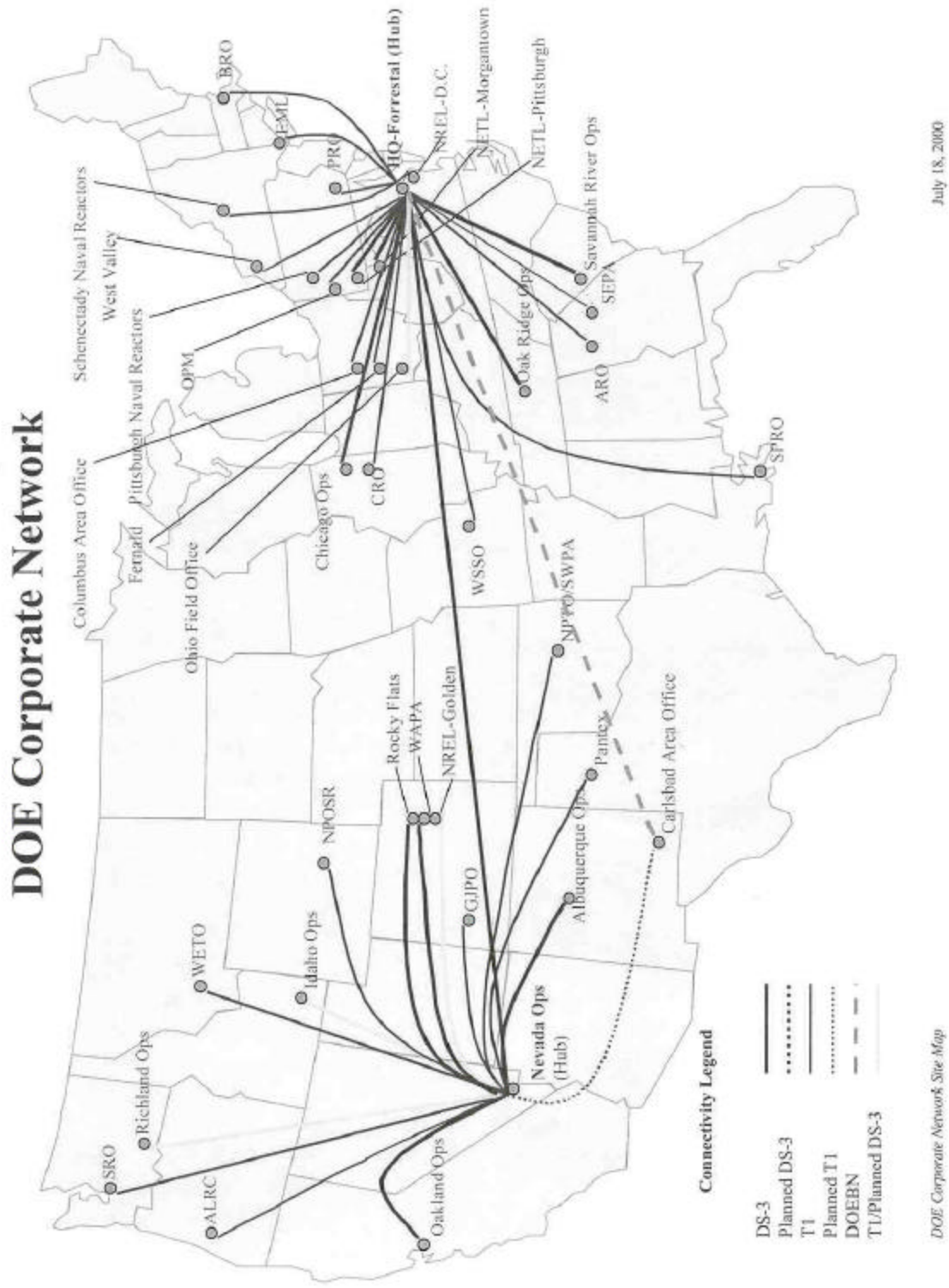
SCOPE

The Office of Inspector General, U.S. Department of Energy, identified a concern relating to the cyber security of unclassified sensitive personal information maintained by the Department under the Privacy Act of 1974 and other personal information exempt from disclosure under the Freedom of Information Act. The OIG announced this inspection in September 2000.

METHODOLOGY

In conducting this inspection, the OIG identified and reviewed applicable Federal and DOE regulations. The OIG interviewed DOE and contractor officials and employees as well as officials from the Office of Management and Budget and the National Institute of Standards and Technology, an agency of the U.S. Department of Commerce's Technology Administration. The OIG also reviewed key documents applicable to the inspection.

Appendix B


DOE Corporate Network
BRO
EML
PRO
HQ-Forrestal (Hub)
NREL-D.C.
NETL-Morgantown
NETL-Pittsburgh
Savannah River Ops
SEPA
ARO
Oak Ridge Ops
SPRO
Schenectady Naval Reactors
West Valley
Pittsburgh Naval Reactors
OPM
Columbus Area Office
Fernald
Ohio Field Office
Chicago Ops
CRO
WSSO
NPOSR
Rocky Flats
WAPA
NREL-Golden
GJPO
Albuquerque Ops
Pantex
Carlsbad Area Office
Idaho Ops
WETO
Richland Ops
SRO
ALRC
Oakland Ops
Nevada Ops
(Hub)
Connectivity Legend
DS-3
Planned DS-3
T1
Planned T1
DOEBN
T1/Planned DS-3
July 18, 2000
DOE Corporate Network Site Map

Appendix C

Department of Energy Corporate Network (DOEnet)

Application Registry
June 2000

Application	Acronym
1. Automated Transportation 2. Management System	ATMS
3. Business Management Information System for Financial Management	BMIS-FM
4. Corporate Human Resource Information System	CHRIS
5. Departmental Integrated Standardized Core Accounting System	DISCAS
6. DOE Integrated Safeguards and Security System	DISS
7. Electronic Commerce	EC Web
8. Energy Time and Attendance	ETA
9. Executive Information System	EIS
10. Frequency Assignment Status	FASTAT
11. Management Analysis Reporting System (MARS)/Financial Information System	MARS/FIS
12. Procurement and Assistance Data System	PADS
13. Primary Organizational Web-Based Employee Records	POWER
14. Safeguards and Security Information Management System	SSIMS
15. WIPP Waste Information System	WWIS

IG Report No.: DOE/IG-0531

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

This page intentionally left blank.

The Office of Inspector General wants to make the distribution of its reports as customer Friendly and cost effective as possible. Therefore, this report will be available Electronically through the Internet at the following alternative address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.