

---

**January 1999**

**GAO FINANCIAL  
MANAGEMENT SYSTEM  
USERS' SECURITY  
MANUAL**

---

---

---

# Contents

---

<b>GAO Financial Management System Users' Security Manual</b>		
	Purpose	2
	FMS Security Requirements	2
	Management's Responsibility for Security	3
	Users' Responsibility for Security	4
	Individual Accountability	5
	General Requirements for FMS Users	5
	FMS Security Policies	6
	Using FMS Data	6
	Using Confidentially Sensitive Data	6
	Accountability	7
	Passwords	7
	Protecting Workstation Availability	7
	Working at Home	7
	Consequences for Failure to Follow Policies	7
<b>Appendixes</b>		
	Appendix I: Contents of GAO'S Financial Management System Security Plan	10
	Appendix II: Major Laws, Regulations, and GAO Policies Affecting GAO'S FMS	12

---

# GAO Financial Management System Users' Security Manual

---

## Purpose

The purpose of this document is to make users of GAO's Financial Management System (FMS) aware of their security responsibilities. This manual describes the sensitivity of FMS data; management's assignment of security responsibility, including user responsibilities; the system's security plan; and the laws and regulations affecting the system. Because of the requirements of these laws and regulations, and because FMS users have access to sensitive GAO data, it is important that each user be aware of these security responsibilities and use this manual to protect GAO's financial system and data. (See appendix I for the contents of the GAO Financial Management System (FMS) Security Plan, which is the basis for this security manual. Appendix II lists and briefly describes the major laws, regulations, and GAO policies that affect GAO's FMS and are the legal and policy basis for the security plan and this security manual.)

The Office of Information Management and Communications' (OIMC) Corporate Systems Center (CSC) has developed and maintains the GAO FMS Security Plan as well as this manual. The FMS System Security Manager, and Alternate System Security Manager, are responsible for ensuring the security of the FMS. The FMS Security Administrator from GAO's Financial Management (FM) office "owns" the information in FMS and decides which privileges users should have. The manager of OIMC's Computer Operations Support Facility (COSF) serves as the FMS Operations Security Administrator and maintains the user identification numbers for accessing the FMS data processing center and the FMS.

---

## FMS Security Requirements

Much of the information used, processed, stored, or transmitted by GAO in FMS is to some degree sensitive. The viability of such a system is based upon three characteristics: data availability, integrity, and confidentiality.

Data availability exists when the data stored in the system are accessible upon demand. Data integrity is the principle that the information contained in the system is complete and precisely what was input into the computer. Data confidentiality is the principle that the computer system limits information disclosure according to the wishes of the owner of the data. The security requirements for FMS are based on the following evaluation of impacts on the system should availability, integrity, or confidentiality be breached.

System characteristics	FMS information security requirements
Availability	Medium sensitivity: The loss of information for several days would not be catastrophic, and, while the cost of recreating the information would be significant, it would not be critical.
Integrity	High sensitivity: If the information were incorrect or modified, government funds might be allocated for unauthorized expenses, and payments might be issued in the wrong amounts or to unauthorized vendors. Since GAO sets the standard for the U.S. government in resource accountability, the system used for internal GAO accounting must meet the highest standards of data integrity.
Confidentiality	Medium sensitivity: FMS contains financial, personal, and proprietary information that must be safeguarded from disclosure to unauthorized personnel. Breach of this responsibility would be embarrassing and potentially costly, but it would not be as critical as a breach of data integrity.

## Management's Responsibility for Security

### System Owner

Richard D. Leland  
OIMC/CSC  
Room 1842  
(202) 512-6645

The System Owner is responsible for ensuring that the security plan is prepared according to prescribed guidelines and is responsible for implementing the plan and monitoring its effectiveness. In addition, the System Owner is responsible for certifying the security controls that are in place for the system.

### System Security Manager

Raymond Bulvin  
OIMC/CSC  
Room 1842  
(202) 512-6647

The duties and responsibilities of the System Security Manager are defined in GAO Order 0510.2, "GAO Information System Security."

---

Alternate System Security  
Manager

Richard D. Leland  
OIMC/CSC  
Room 1842  
(202) 512-6645

The Alternate System Security Manager acts in the System Security Manager's absence.

FMS Security Administrator

Sylvia Dickens  
FM  
Room 6T37  
(202) 512-3274

The FMS Security Administrator is responsible for determining FMS user security profiles.

Operations Security  
Administrator

Computer Operations Support Facility Manager  
COSF  
Room 1130  
(202) 512-3043

The Operations Security Administrator is responsible for establishing security access for new FMS users and modifying existing access as necessary for security purposes.

---

## Users' Responsibility for Security

All GAO staff have a security background investigation after they are hired that is based on their position designations. Positions that involve FMS use or maintenance have been designated "public trust" positions. These positions are assigned levels of risk—low, moderate, or high—according to GAO Notice 0910.1, "Position Description Designation Procedure." Employees in low-risk positions have an initial National Agency Check with Inquiries and Credit (NACIC) investigation, which is updated every 10 years. Moderate-risk positions require an initial NACIC investigation, followed by an update every 7 years. OIMC staff who maintain FMS fall into this category. High-risk positions require an initial background investigation, which is updated every 5 years. Employees in high-risk positions are not allowed access to FMS until the background investigation is completed.

---

## Individual Accountability

Individual accountability for FMS is accomplished by issuing appropriate individuals two unique numbers: an FMS data processing center user identification number and an FMS user identification number, both of which are needed to enter the system. It is possible in this way to associate users with their FMS-related actions.

GAO's policy is to assign access privileges on the basis of "least privilege"; that is, users are given the minimum level of access necessary to perform their job functions. Working within FMS can involve processing documents; approving documents; and viewing, adding, changing, or deleting information. Employees with document processing access, for example, process documents but do not approve the documents they have processed. Employees with approving authority access can add, change, delete, or override information entered in FMS documents.

---

## General Requirements for FMS Users

- Attend an FMS security briefing.
- Be familiar with all security policies and practices involving FMS, especially those for confidentially sensitive information. Comply with these policies and practices.
- Be aware of and comply with GAO Order 0510.2, "GAO Information Systems Security."
- Be aware of the identities, roles, and responsibilities of the FMS System Owner, FMS System Security Manager, Alternate System Security Manager, FMS Security Administrator, and Operations Security Administrator.
- Use only FMS data that are necessary to perform assigned duties and report failures in the system's access control to supervisory personnel.
- Never attempt to circumvent or defeat security safeguards and countermeasures established for the protection of FMS and the FMS data processing center.
- Maintain security for FMS by correctly using established security mechanisms and practices when using FMS on the GAO LAN.
- Report security-related events to supervisors, the System Security Manager, the FMS Security Administrator, or the Operations Security Administrator. Security-related events include security infractions by coworkers, attempted access by unauthorized personnel, violations of procedures, disclosure of sensitive information, loss of availability of FMS resources, destruction of data, and detection of erroneous information or unexplained system activity.
- Notify the FMS Security Administrator when staff terminate or change positions so that system access privileges can be adjusted accordingly.

---

## FMS Security Policies

This section contains specific rules of behavior to be followed to implement GAO's policies for maintaining FMS Security.

---

### Using FMS Data

- Do not attempt to view, change, or delete data unless you are authorized to do so.
- Do not use your system privileges to obtain data or files or to run applications for anyone who does not have authorized access to the system.
- Strive for 100-percent accuracy during data input and correct any inaccurate data.
- Control access to your PC and log out of FMS whenever you leave your machine.
- Use a screen saver with a password. Set the screen saver to display after 5 minutes of inactivity.

---

### Using Confidentially Sensitive Data

- Be sure that only authorized personnel are allowed to view confidential data, whether the data are on your screen or on paper.
- Never discuss sensitive information with unauthorized personnel. Never discuss such information with authorized personnel over the phone or in an area where you might be overheard. This is especially important for personal action information subject to the Privacy Act. Shred confidentially sensitive documents.
- Safeguard sensitive hard-copy data.
- When copying sensitive FMS data to a disk or other electronic medium, label it to indicate that it contains sensitive data that should not be disclosed to unauthorized personnel.
- When viewing or processing confidentially sensitive data, be sure the PC is in an isolated area and that only people authorized to see the data are present.
- When printing hard-copy reports containing sensitive data on a printer that is accessible to unauthorized personnel, pick up the printed material quickly to ensure data are not seen or obtained by unauthorized personnel.
- Never remove sensitive FMS data from GAO without the approval of supervisory personnel.
- Position workstation/computer screens away from doors, windows, and heavily traveled areas.
- If you see an unfamiliar person in an area where sensitive FMS data are used or stored, challenge him or her immediately to prevent inappropriate access to sensitive data.

---

## Accountability

- Do not attempt to perform actions or processing for which you do not have authorization.
- Be alert to threats to FMS and its data.

---

## Passwords

- Follow all password guidance for using the GAO LAN.
- Change your FMS data processing center password every 30 days. Do not reuse the same password.
- Use at least six characters in your FMS password.
- Use a mix of alpha and numeric characters; do not use family names, birthdays, sports teams, words that can be found in the dictionary, or words that can be associated with the user's personality or possessions.
- Safeguard passwords and user account numbers from other personnel; do not reveal them either orally or in writing.
- Memorize your password; if you write it down, keep it in a secure place.

---

## Protecting Workstation Availability

- Follow all virus protection procedures set forth in GAO's Securing Information in Today's Computer Environment. Know how to use virus scanning software, and do not use disks from other machines without first scanning them.
- Log out and turn off your PC when you leave the facility.
- Protect machines from hazards such as food, drink, smoke, water, and excessive heat.
- Ensure that individual workstations and peripheral devices are connected to a surge suppressor or other power protection device.
- Never connect to other networks or hosts without permission of supervisory or security personnel.
- Use GAO automated systems for official purposes only.

---

## Working at Home

- Use government equipment for official purposes only.
- Take precautions to secure government information and information resources.
- Follow all provisions of employer/employee agreements related to off-site work.

---

## Consequences for Failure to Follow Policies

All FMS users must ensure that the system and its data are protected from loss, misuse, and unauthorized access or modification. This means that all users are responsible for protecting confidentially sensitive data from unauthorized or accidental disclosure and are responsible and

accountable for their use of the system and its data . Failure to follow the policies for FMS use that are listed in this manual may result in one or more of the following actions:

- suspension of access privileges,
- reprimand,
- demotion,
- suspension, or
- removal.

In addition, for certain infractions—especially for the unauthorized disclosure of confidentially sensitive data—criminal or civil penalties, including fines, prison terms, or both, may be imposed. The severity of the action is determined at the discretion of management, through due process of law, on the basis of the seriousness of the violation. These consequences are described in GAO Order 2751.1 Personnel Supplement.

---

---

# Contents of GAO'S Financial Management System Security Plan

This Appendix lists the contents of the GAO Financial Management System (FMS) Security Plan, which is the basis for this security manual. Refer to it for additional information about FMS security.

I. SYSTEM IDENTIFICATION	1
I.A. Responsible Organization	1
I.B. System Name	1
I.C. System Category	1
I.D. System Operational Status	1
I.E. General Description/Purpose	1
I.F. System Environment and Special Considerations	3
I.G. System Interconnection/Information Sharing	3
I.H. Information Contacts	4
II. SENSITIVITY OF INFORMATION HANDLED	5
II.A. Applicable Laws or Regulations Affecting the System	5
II.B. General Description of Sensitivity	6
III. SYSTEM SECURITY MEASURES	8
III.A. Risk Assessment and Management	8
III.A.1. Background	8
III.A.2. Methodology	9
III.A.3. Findings	9
III.A.4. Conclusions	10
III.B. Review of Security Controls	16
III.C. Applicable Guidance	16
III.D. Rules of Behavior	17
III.D.1. FMS Application User Responsibilities	18
III.D.2. Application User Rules	18
III.D.3. FMS Application Maintenance and Operations	
Staff Rules	22
III.E. Security Control Measures	22
III.E.1. Management Controls	22
III.E.1.a. Assignment of Security Responsibility	22
III.E.1.b. Personnel Security	23
III.E.2. Development/Implementation Controls	24
III.E.2.a. Authorize Processing	24
III.E.2.b. Security Specifications	25
III.E.2.c. Design Review and Testing	25
III.E.3. Operational Controls	25
III.E.3.a. Physical and Environmental Protection	25
III.E.3.b. Production, Input/Output Controls	26

---

**Appendix I**  
**Contents of GAO'S Financial Management**  
**System Security Plan**

---

III.E.3.c. Contingency Planning	28
III.E.3.d. Audit and Variance Detection	28
III.E.3.e. Application Software Maintenance Controls	28
III.E.3.f. Documentation	29
III.E.4. Security Awareness and Training	30
III.E.4.a. Security Awareness and Training Measures	30
III.E.5. Technical Controls	31
III.E.5.a. User Identification and Authentication	31
III.E.5.b. Authorization/Access Controls	32
III.E.5.c. Public Access Controls	33
III.E.5.d. Data Integrity/Validation Controls	34
III.E.5.e. Audit Trail Mechanisms	34
III.E.6. Complementary Controls Provided by Support Systems	35
IV. ADDITIONAL COMMENTS	36
Appendix A - FMS Risks Countermeasures Action Plan	37

---

# Major Laws, Regulations, and GAO Policies Affecting GAO'S FMS

---

Privacy Act of 1974, P.L. 93-579	<p>This act requires the U.S. government to safeguard personal data processed by federal agency computer systems. The act assigns two basic areas of responsibility to federal agencies and employees:</p> <ul style="list-style-type: none"><li>• maintaining the confidentiality of data covered by the act and</li><li>• taking those actions necessary to reasonably ensure that data concerning individuals maintained in federal information systems are accurate.</li></ul>
	<p>Failure to comply with the provisions of the act could make the agency and individuals within the agency liable for criminal and civil penalties.</p>
Federal Managers' Financial Integrity Act of 1982, P.L. 97-255	<p>The basic objective of the act is to reduce or eliminate the incidence of waste, fraud, and abuse in government financial systems.</p>
Computer Fraud and Abuse Act of 1986, P.L. 99-474	<p>This act prohibits unauthorized remote access to, or modification of information in, computer systems containing national defense, banking, or financial information.</p>
Computer Security Act of 1987, P.L. 100-235	<p>This act requires computer security plans for all federal computer systems that contain sensitive information and requires computer security awareness training of all individuals involved in the management, use, or operation of federal computer systems that contain sensitive information.</p>
OMB Circular No. A-127, "Financial Management Systems"	<p>This circular sets policy for the Federal Managers' Financial Integrity Act.</p>
OMB Circular No. A-130, "Security of Federal Automated Systems," Appendix III	<p>This circular establishes a minimum set of controls to be included in Federal automated information security programs and incorporates requirements of the Computer Security Act of 1987.</p>
GAO Order 0510.2, "GAO Information System Security"	<p>This order defines policies and standards for security of unclassified information systems. The order assigns responsibilities and accountability for providing reasonable assurance that GAO's information systems' resources are protected against fraud, waste, abuse, disaster, and mismanagement.</p>

---

**Appendix II**  
**Major Laws, Regulations, and GAO Policies**  
**Affecting GAO'S FMS**

---

The order defines each GAO employee's responsibility to

- follow the security policies and procedures detailed in the order and the GAO Security Manual and those security policies and procedures issued by local management and
- promptly report to local management or the appropriate accreditation authority any fraud, waste, abuse, inadvertent disclosure, or compromise associated with an information system.

---

**GAO Pamphlet "Securing  
Information in Today's  
Computer Environment"**

This pamphlet addresses

- the risk associated with GAO's computer environment,
- staff's security responsibilities regarding information systems, and
- actions that promote good security practices.

---

## Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are \$2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. 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

### or visit:

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

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or 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.

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](mailto:info@www.gao.gov)

or visit GAO's World Wide Web Home Page at:

<http://www.gao.gov>

---

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

**Bulk Rate  
Postage & Fees Paid  
GAO  
Permit No. G100**

**Official Business  
Penalty for Private Use \$300**

**Address Correction Requested**

---

