United States General Accounting Office 145147

GAO

Office of Security and Safety

SP-049

April 1991

Security Highlights

Introduction

This publication has been prepared by the Office of Security and Safety (OSS) to introduce employees to GAO Order 0910.1, The GAO Security Manual. It is designed to acquaint employees with their security responsibilities and the requirements of the Manual, but does not attempt to cover or summarize material found in the Manual.

This publication is divided into security subject areas that correspond to the major topics addressed in the Manual. To enable readers to easily find information of interest in the Manual, parenthetical references to the Manual's page numbers have been included. The "Do's and Don'ts" listed in this publication are just some, not all, of the points discussed in the Manual. They are included here to promote security awareness. Each employee should read that part of the Manual which deals more fully with the concerned subject area.

The GAO Security Manual

The GAO Security Manual is a comprehensive, single-source, reference document that details GAO security policy and procedures. It defines the elements of GAO's Security Program: Information Security, Personnel Security, Physical Security, Classified Computer and Communications Security, and Industrial Security. The Manual applies to all employees, consultants, contractors, and other persons granted access to GAO information, property, or areas controlled by GAO. Unit Local Security Officers and Administrative Officers maintain copies of the Manuals at their offices. Employees are required at all times to be knowledgeable of those segments of the Manual pertinent to their duties. Failure to adhere to the rules and procedures set forth in the Manual may seriously impact GAO; violations of the regulations may result in civil, criminal, or administrative sanctions.

General

Security is an operational activity concerned with the safeguarding of information, property, and personnel. GAO's Security Program comprises security policy and procedures promulgated by a central GAO office (OSS) and implemented by unit (division/office) management. Each GAO division and office has designated a Local Security Officer who assists local management in carrying out the security program to maintain the integrity of areas, information, and property under GAO control. Employees should seek guidance and assistance from their Local Security Officer to ensure that personal obligations under the GAO Security Program are being met. OSS is available for additional assistance on (202) 275-4700.

Contents

Chapter 1

Information Security and Classified National Security Information

Background

Information Security is that area of security concerned with identifying and protecting information that warrants protection in the national interest. Chapter 1 of The GAO Security Manual covers the basic elements of GAO's Information Security Program dealing with classified information.

Subject Areas Covered in Chapter 1 of the GAO Security Manual

Information security policy (pp. 1-1 thru 1-3).

Program management (pp. 1-3 thru 1-5).

Classification principles and considerations (pp. 1-5 thru 1-11).

Markings (pp. 1-11 thru 1-17).

Control and accountability (pp. 1-18 thru 1-23).

Custody and safeguarding (pp. 1-23 thru 1-28).

Transmission of classified information (pp. 1-29 thru 1-34).

Access and dissemination (pp. 1-40 and 1-41).

Destruction of classified material (pp. 1-40 and 1-41).

Loss or compromise of classified information (pp. 1-41 thru 1-43).

SOME Information Security Do's and Don'ts

General

- Know the requirements for access to and handling of classified and/or unclassified sensitive information (pp. 1-1 and 1-2).
- Properly mark all GAO-produced documents (pp. 1-2, 1-5, 1-11 and 1-12).
- Log-in all classified materials (p. 1-20).
- Promptly report actual or suspected compromises of classified information (p. 1-41).
- Properly destroy classified information when no longer needed (pp. 1-40 and 1-41).
- Report any contact with persons from the countries listed in appendix 4 of The GAO Security Manual (p. 1-29).

Safeguarding

- Cover classified documents with appropriate cover sheets when not in a security container (pp. 1-12 and 1-26).
- Don't declassify or release classified information without proper authorization (pp. 1-2, 1-3, 1-7, 1-8, 1-10 and 1-11).
- Don't write combinations down (p. 1-25).
- Don't read or display classified information in public places (p. 1-31).

Transmission

- Use proper procedures to transmit Secret and Confidential information (pp. 1-30 and 1-31).
- Obtain receipts when transmitting classified information (pp. 1-33 and 1-34).
- Don't discuss classified information over the telephone or where it may be heard by unauthorized persons (p. 1-23).
- Don't mail Top Secret information (p. 1-29).
- Don't take classified information home (p. 1-31).
- Don't take classified information into foreign countries (p. 1-32).

- Don't fax classified information (p. 1-34).
- Don't provide classified information to unauthorized persons (p. 1-36).

Special Category Classified and Other Controlled Information

Background

Some classified information may require special access authorizations (classified NATO and nuclear information) and/or safeguarding by methods different than that for other classified information. Also, certain unclassified information may require special handling and protection from unauthorized disclosure due to its sensitive nature.

Subject Areas Covered in Chapter 2 of the GAO Security Manual

North Atlantic Treaty Organization (NATO) Information (pp. 2-1 thru 2-7).

"Internal GAO Use Only", "For Official Use Only", "Limited Official Use", "Privacy", "Unclassified Nuclear", "Medical", and "Private Employee Benefit Plan Information" (pp. 2-8 thru 2-15).

Tax Information (pp. 2-16 thru 2-21).

Restricted Geological or Geophysical Information (pp. 2-21 thru 2-25).

Nuclear Information (pp. 2-25 thru 2-31).

Procurement Sensitive Information (pp. 2-31 thru 2-35).

SOME Information Security Do's and Don'ts

NATO Information

- Safeguard and store properly (p. 2-1 thru 2-7).
- Read United States Security Authority for NATO (USSAN) Instruction 1-69 (p. 2-1).
- Return NATO documents properly (pp. 2-5 and 2-6).
- Change combinations on time (p. 2-7).
- Know special requirements for NATO Top Secret information (a.k.a. COSMIC) (p. 2-6).
- Don't reproduce NATO documents (p. 2-6).
- Don't mix NATO and non-NATO material (p. 2-7).
- Don't destroy NATO material (p. 2-7).
- Know what to do with NATO classified material in emergency situations (p. 2-7).

"Internal GAO Use Only", "For Official Use Only", "Limited Official Use", "Privacy", "Unclassified Nuclear", "Medical", and "Private Employee Benefit Plan Information"

- Prevent disclosure to unauthorized persons (p. 2-9).
- Store properly (p. 2-9).
- Mark properly (pp. 2-11 thru 2-14).
- Use cover sheets (p. 2-9).
- Dispose of properly when no longer needed (p. 2-11).
- Promptly report unauthorized disclosures (p. 2-15).
- Don't mail "For Official Use Only" or "Limited Official Use" material through foreign postal systems (p. 2-10).
- Don't display or discuss around unauthorized persons (p. 2-10).
- Don't carry across foreign borders (p. 2-10).

Tax Information

- Know GAO Order 0135.1 and sections 7431 and 7213(a) of the Internal Revenue Code (p. 2-16).
- Disclose only to authorized individuals and promptly report unauthorized disclosures (pp. 2-16 and 2-17).
- Safeguard properly (pp. 2-17 thru 2-21).
- Mark properly (p. 2-19).
- Know how to properly transmit tax information (p. 2-19).
- Discuss tax information over secure telephone circuits only (p. 2-19).
- Know the procedure for transferring tax information that is no longer needed (p. 2-19).
- Work with tax information in special areas only (p. 2-20).

Restricted Geological or Geophysical Information (RGGI)

- Know GAO Order 0940.2 (p. 2-22).

- When discussing RGGI with authorized persons, advise them that the information is RGGI (p. 2-22).
- Report unauthorized disclosures (pp. 2-22 and 2-23).
- Secure when not in use (p. 2-24).
- Destroy by shredding when no longer needed (p. 2-25).
- Don't display or talk about RGGI around persons who aren't entitled to the information (p. 2-22).

Nuclear Information

- Know the pertinent U.S. Department of Energy and Nuclear Regulatory Commission regulations (p. 2-25).
- Know requirements for storing Restricted Data (RD) and Formerly Restricted Data (FRD) (pp. 2-29 and 2-30).
- Know requirements for access (p. 2-31).
- Immediately report all missing classified material containing RD or FRD (p. 2-31).
- Don't discuss or release unclassified nuclear information to unauthorized persons (pp. 2-26 and 2-27).

Procurement Sensitive Information

- Properly secure procurement sensitive information when not in use (p. 2-33).
- Report unauthorized disclosures to local unit management immediately (p. 2-34).
- Use a cover sheet when working with procurement sensitive information (p. 2-34).
- Shred when no longer needed (p. 2-34).
- Don't discuss or display procurement sensitive information around unauthorized individuals (p. 2-33).

Chapter 3

Personnel Security

Background

Personnel Security is that area of security concerned with the standards and procedures for determining whether an individual's employment or retention is clearly consistent with national security interests. It encompasses not only an individual's loyalty to the United States, but also personal habits, character, associations, reliability, judgement, susceptibility to coercion, and other areas of security significance.

Subject Areas Covered in Chapter 3 of the GAO Security Manual

Protection and dissemination of personnel security information (pp. 3-3 and 3-4).

Position sensitivity (pp. 3-4 thru 3-6).

Investigative requirements (pp. 3-6 thru 3-8).

Operational responsibilities of the Director, OSS (pp. 3-9 and 3-10).

Authorizations for access to classified information (pp. 3-10 thru 3-12).

Administrative withdrawal of security clearances (pp. 3-12 and 3-13).

Security briefings and debriefings (pp. 3-13 and 3-14).

Special access authorizations (pp. 3-14 and 3-15).

Office of Personnel responsibilities (pp. 3-15 and 3-16).

Responsibilities of units, heads of divisions and offices, Local Security Officers, employees, and the Director of the Office of Recruitment (pp. 3-16 thru 3-19).

Special employment and exchange programs (pp. 3-20 thru 3-22).

Guidelines for suitability referral (pp. 3-22 and 3-23).

Criteria for determining eligibility for access to classified information (pp. 3-23 thru 3-26).

Procedures for resolving questions of eligibility for a security clearance (pp. 3-26 thru 3-38).

Security Adjudication Committee (pp. 3-32 thru 3-38).

SOME Personnel Security Do's and Don'ts

- Report adverse information to appropriate officials (p. 3-2).
- Properly secure all information of a personal or privileged nature (p. 3-4).
- Submit updated personnel security paperwork to the proper official on time (p. 3-8, 3-11 and 3-12).
- Attend security briefings and debriefings when required (pp. 3-13 and 3-14).
- Don't give access to classified information to those who haven't been properly briefed and authorized for access (p. 3-14).
- Don't confuse employment suitability with clearance eligibility (p. 3-22).
- Avoid conduct which can affect one's clearance eligibility or suitability (pp. 3-22 thru 3-25).

Chapter 4

Physical Security

Background

Physical Security is that area of security concerned with physically safeguarding personnel, property, and information. The main object of physical security is to make access as difficult as possible to deter an intruder from trying to gain entry or access, and to facilitate the apprehension of anyone who does try.

Subject Areas Covered in Chapter 4 of the GAO Security Manual

Types and uses of protective barriers (pp. 4-2 and 4-3).

Protective lighting (p. 4-3).

Controls and techniques to control the movement of people (pp. 4-3 and 4-4).

Alarm systems to detect entry into a controlled area (pp. 4-5 and 4-6).

The use of locks, locking devices, and key control (pp. 4-6 and 4-7).

Security containers and safes, changing combinations, required forms and other controls (pp. 4-7 thru 4-10).

Vaults and strongrooms (p. 4-10).

Guard forces and guard coverage arranged by GAO (p. 4-10).

Contingency planning for disasters (p. 4-11).

Bomb threats (pp. 4-11 and 4-12).

Preventing pilferage in the work place (p. 4-12).

Terrorism (pp. 4-13 and 4-14).

The property pass system (pp. 4-14 and 4-15).

Vehicle parking and its role in security (pp. 4-15 and 4-16).

GAO identification documents (ID) (pp. 4-16 thru 4-18).

What to do if GAO ID are lost or stolen (pp. 4-20 and 4-21).

How GAO ID are stored, transmitted and accounted for (p. 4-21).

Using GAO official credentials (p. 4-22).

SOME Physical Security Do's and Don'ts

Locks, Security Containers and Safes

- Use only GAO-issued locks and containers appropriate for the material to be stored (pp. 4-6 thru 4-8).
- Report evidence of tampering with locks and locking devices (p. 4-7).
- Use proper forms on security containers (pp. 4-9 and 4-10).
- Secure valuables when left unattended and secure offices, desks, and file cabinets before leaving for lunch, the restroom, or at the end of the workday (p. 4-12).
- Don't store cash and/or valuables with classified material (p. 4-8).

Combinations

- Change combinations when they are supposed to be changed, and use the proper procedures (pp. 4-8 and 4-9).
- Don't write combinations down (p. 4-8).

Key Control

- Turn in all GAO-issued keys when no longer needed (p. 4-7).
- Don't reproduce GAO-issued keys (p. 4-7).

Bomb Threats, Terrorism and Contingency Plans

- Take all bomb threats seriously (p. 4-11).
- Properly report and respond to bomb threats or terrorist acts (pp. 4-11 thru 4-14).
- Secure classified information before vacating the premises (pp. 4-11 and 4-13).
- Know office contingency plans and employee responsibilities in the event of an emergency (p. 4-11).

ID Media

- Use GAO ID for official purposes only (p. 4-18).
- Report any unauthorized use of GAO ID (p. 4-21).
- Safeguard GAO ID against loss, theft or damage, and report lost or stolen ID (p. 4-21).
- Report recoveries of GAO ID (pp. 4-20 and 4-21).
- Turn in all GAO ID when no longer needed (p. 4-20).
- Don't use access badges in automated access control systems if the badges are damaged or have been reported missing (p. 4-21).
- Don't lend GAO ID to any other person for any purpose (p. 4-21).
- Don't place GAO ID used in automated access control systems next to any other magnetic-stripe card (p. 4-21).

NOTE: OSS also distributes a separate pamphlet on the proper use and handling of GAO ID.

Chapter 5

Industrial Security

Background

Industrial Security is an area of security concerned with protecting classified information in the hands of United States industry.

Subject Areas Covered in Chapter 5 of the GAO Security Manual

Operation of GAO's Industrial Security Program (pp. 5-1 and 5-2).

Releasing classified information to GAO contractors (pp. 5-2 and 5-3).

Reporting unauthorized disclosures (p. 5-3).

Security Requirements Clause for classified contracts (p. 5-3).

GAO's agreement with the Department of Defense concerning the Defense Industrial Security Program (pp. 5-4 and 5-5).

SOME Industrial Security Do's and Don'ts

- Immediately notify the Director, OSS, if classified information may be required during precontract negotiations (p. 5-2).
- Put a security requirement clause in classified contracts (p. 5-3).
- Know the procedure for handling classified material marked "Not Releasable to Contractors" (p. 5-2).
- Don't allow contractors without proper clearance and need-to-know to have access to classified information (pp. 5-1 and 5-2).