SECURITY STANDARD OPERATING PROCEDURES

TABLE OF CONTENTS

CHAPTER 7. SUBCONTRACTING

CHAPTER 8. AUTOMATED INFORMATION SYSTEM SECURITY

CHAPTER 9. SPECIAL REQUIREMENTS

CHAPTER 10. INTERNATIONAL SECURITY REQUIREMENTS

CHAPTER 11. MISCELLANEOUS INFORMATION

APPENDICES

INTRODUCTION

1. Purpose. To provide our Government Customer with a set of Standard Operating Procedures that will ensure that EG&G is in compliance with the safeguarding of classified information in accordance with the applicable Government guidelines.

2. Ogranizational Units Concerned. All EG&G employees and consultants.

3. Responsibilities.

a. Manager, Security Services is responsible for the development and overall management of the security program for all EG&G facilities.

b. Facility Security Officer (FSO) is responsible for implementing and administering their industrial security program as prescribed in the NISPOM and in these SOPs and any approved addendum to the SOPs.

c. Managers and Supervisors are responsible for the observance of security measures affecting their respective organizations and the employees under their supervision. Access to classified information or material will be limited to those employees who have a need to know and are capable of protecting the information or material. Uncleared personnel will be assigned duties which do not permit access to classified information.

d. Employees granted access to classified material are responsible for its protection when accountable to them or in their control. They will also be responsible for safeguarding any classified information that may come to their knowledge or possession while in the discharge of their assigned duties.

In addition to each individual's continuing responsibility to safeguard classified information, a need exists for all employees, particularly those with supervisory responsibilities, to promptly report any ADVERSE INFORMATION to the FSO. As a general rule, any information which reflects adversely upon the integrity or general character of an employee or which indicates that the person's ability to safeguard classified information may be impaired, should be reported. Information provided will be safeguarded, provided the highest degree of protection, and handled as sensitive personal information.

SECURITY STANDARD OPERATING PROCEDURES

The Security Standard Operating Procedures dated 31 March 2000 is approved in its entirety.

Approved: _____
Bernard VanderWeele
Security Manager/FSO

Approved: _____
Gary H. Fitzgerald
President

Approved: _____
Roger Lackens
PSO

31 March 2000

CHAPTER 1. GENERAL PROVISIONS AND REQUIREMENTS

Section 1. Purpose and Scope.

1-100. Purpose. To establish security standard operating procedures (SOP) and place into effect all controls required to safeguard classified information in accordance with the National Industrial Security Program Operations Manual (NISPOM), and to provide special security measures to ensure the integrity of Special Access Programs (SAP) in accordance with the NISPOMSUP.

a. This SOP incorporates supplemental special security measures to ensure the integrity of EG&G Special Access Programs (SAPS) and other classified collateral programs. These SOPs will meet the requirements of the appropriate DD254 , Program Security Guide, and the NISPOMSUP.

1-101. Scope.

a. These SOPs apply to all EG&G employees and are used to safeguard all classified information released to or generated by EG&G in the course of contract performance.

1. This document is applicable to all SAP contracts.

b. DCID 1/21 will apply to all SCI and SAP programs as the security measures at this facility.

1-102. Agency Agreement SAP Program Areas.

a. The Government Agency establishing the SAP will appoint a Government Program Security Officer (PSO) who will be responsible for security of the program and all program areas.

b. Department of Defense (DOD)/Defense Security Services (DSS) still has security cognizance, but defers to SAP controls per agency agreements.

1-103. Security Cognizance.

a. The DOD and Government Customer PSO will have security cognizance over EG&G SAP programs and DOD Cognizant Security Office will have cognizance over all collateral programs.

1-104. Interpretations. All requests for interpretation of the NISPOM will be forwarded to the CSA through its designated CSO.

a. All requests for interpretations of the NISPOMSUP will be forwarded to the SAP PSO.

1-105. Supplement Changes. Recommended changes and comments will be submitted through the PSO.

1-106. Waivers and Exceptions. Requests shall be submitted through Government channels approved by the CSA. Waivers and Exceptions will not be granted to impose more stringent protection requirements than the NISPOM provides for Confidential, Secret or Top Secret information.

a. Requests for waivers will be submitted to the PSO on a SAPF 12. Waivers will be requested only if they are in the best interest of the Government.

1-107. Special Access Programs Categories. There are four generic categories of SAPs: Acquisition SAP (AQ-SAP); Intelligence SAP (IN-SAP); Operations and Support SAP (OS-SAP); SCI Programs (SCI-SAP). There are two types of SAPs:

a. ACKNOWLEDGED: Acknowledged SAP is a program which may be openly recognized or known; however, specifics are classified within that SAP.

b. UNACKNOWLEDGED: Unacknowledged SAP will not be made known to any person not authorized for this information.

Section 2. General Requirements. As a contractor to the Department of Defense (DOD) EG&G Technical Services has executed a security agreement which provides authorization for access to classified information and materials. Included as a part of this agreement are the terms and conditions by which we must administer a program to provide acceptable levels of security control. These Standard Operations Procedures (SOP) have been prepared to implement the procedures necessary to safeguard classified material.

1-200. Responsibilities.

a. The Contractor Program Manager (CPM) will be appointed by company management and will be responsible for:

1. Overall Program management.

2. Execution of the statement of work, contract, task orders and all other contractual obligations.

b. The Contractor Program Security Officer (CPSO) will be the company Security Manager/Facility Security Officer (FSO) and will oversee compliance with SAP security requirements. The CPSO/FSO will:

1. Possess a personnel clearance and Program access at least equal to the highest level of Program classified information involved.

2. Provide security administration and management for his/her organization.

3. Ensure personnel processed for access to a SAP meet the prerequisite personnel clearance and/or investigative requirements specified.

4. Ensure adequate secure storage and work spaces.

5. Ensure strict adherence to the provisions of the NISPOM, its Supplement Overprint.

6. When required, establish and oversee a classified material control program for each SAPF.

7. When required, establish and oversee a classified material control program for each SAP.

8. When required, establish a SAPF.

9. Establish and oversee visitor control program.

10. Monitor reproduction and/or duplication and destruction capability of classified information.

11. Ensure adherence to special communications capabilities within the SAPF.

12. Provide for initial Program indoctrination of employees after their access is approved; rebrief and debrief personnel as required.

13. Establish and oversee specified procedures for the transmission of classified material to and from 821 Grier Drive.

14. Ensure contractual specific security requirements such as TEMPEST, AIS and OPSEC are accomplished.

15. Establish security training and briefings specifically tailored to the unique requirements of the SAP.

1-202. Standard Operating Procedures (SOPs). SOPs will be prepared by the CPSO and forward to the PSO for approval. SOPs will be reviewed at least annually by the CPSO unless changes require immediate action. All changes will be reported to the PSO as they occur.

1-203. Badging.

Identification Badging.

a. A permanent badge will be issued to the employee by the Security Office on the first day of employment.

b. Select customers who have a continuing need for access to program areas and personnel will be issued permanent badges by the Security Office.

c. Badges shall be promptly recovered, or when appropriate, re-issued whenever an employee's/customer's requirement for entry to a program area no longer exists due to an internal transfer, termination of employment, or for other appropriate reasons.

Badge Preparation.

a. The Security Office prior to badge preparation will make verification of clearance and required area access.

b. A color photograph is then made of the badge recipient and through the use of a "mug board," the individuals last name and employee number appears on the picture. Customer photographs will be identified by the last four digits of their social security number.

c. Badge insert is laminated; badge number; date of issue and recipient's name is then recorded in the badge log.

d. Badges must be worn on the outer garment, above the waist. Necklaces are acceptable for display of badges, should the wearer choose.

Control/Accountability. A system for badge control and accountability is in force.

a. All Permanent badge blanks are individually numbered with a sequential number on the front.

b. Permanent badges are recorded in a master log, using the preprinted sequential number on the front, date of issue and printed name.

c. Visitor badges are maintained at the Access Control Officer's station.

d. All visitor badges are individually numbered and are issued to individuals on official business with EG&G Technical Services.

e. The type of badge issued is determined by the purpose of the visit and verified clearance level. Upon issue, the badge number is recorded on the visitor log.

f. On departure from the facility, badges will be returned to the Access Control Officer and the departure time is recorded on the visitor log. Badges are checked to insure the individual has returned the same badge issued.

Card Access. In addition to the identification badges worn by all employees Card readers are on all cleared area doors. These access cards are issued to those cleared individuals working in those project areas or in the cleared area of the building.

a. Access Cards are issued and accounted for in the MDI database.

b. The Security Office prior to card preparation will make verification of clearance and required area access.

Badge Information.

a. **Colors.**

EG&G Technical Services Employees	Black Top Section
Sub-contract employees/Temporary employees	Blue Top Section
Customers and Government Reps/ Consultants	Purple Top Section
Cleared Visitors Badges	Red Top Section
Uncleared Visitors, Escort Required	Orange Top Section

b. **Color Bar Coding.**

Yellow Bar	Top Secret + Access
Orange Bar	Top Secret
Red Bar	Secret
Green Bar	No Security Clearance

1-204. COMSEC. Classified SAP information will be electronically transmitted only by approved secure communication channels authorized by the PSO. Details are provided in Chapter 11.

1-205. Two-Person Integrity (TPI). TPI rule may be required in program areas with Program CSA approval. This requirement does not apply to those situations where one employee with access is left alone for brief periods of time, nor dictate that those employees be in view of one another.

1-206. Contractor's Questioning Perceived Excessive Security requirements. All personnel are highly encouraged to identify excessive security measures that they believe have no added value or are cost excessive and should report this information to their industry contracting officer for subsequent reporting through contracting channels to the appropriate PSO.

1-207. Security Reviews and Self Inspections. Security reviews will be conducted by both DSS and PSO on at least an annual basis.

a. Self Inspections will be conducted by EG&G Security Department semi-annually, unless required more frequently.

1-208. Cooperation with Federal Agencies. EG&G shall cooperate with Federal agencies during official inspections, investigations concerning the protection of classified information, and during the conduct of personnel security investigations of present or former employees and others. This includes providing suitable arrangements within the facility for conducting private interviews with employees during normal working hours, providing relevant employment and security records for review, when requested, and rendering other necessary assistance.

1-209. Fraud, Waste & Abuse. (FWA) Government and Industry FWA reporting is encouraged through channels designated by the PSO. Do not use other advertised FWA hotlines when program or SAP information may be reviewed. Contact the Security Manager for the telephone number of the current FWA manager.

Section 3. Reporting Requirements

1-300. General. EG&G Technical Services will submit a formal written report to the CSO, with copies to the PSO as directed by Section 3, Chapter 1 of the NISPOM, on the following subjects, as required:

1-301. Reports to be Submitted to the FBI. A written report shall be promptly submitted to the nearest field office of the FBI, regarding information coming to the contractor's attention concerning actual, probable or possible espionage, sabotage, or subversive activities at any of its locations. An initial report may be made by phone, but

it must be followed in writing, regardless of the disposition made of the report by the FBI. A copy of the written report shall be provided to the CSA.

1-302. Reports to be Submitted to the CSA.

a. **Adverse Information.** A report shall be submitted on any adverse information concerning any cleared employees. The report shall include the name and telephone number of the individual to contact for further information regarding the matter and the signature, typed name and title of the individual submitting the report.

b. **Suspicious Contacts.** Any effort by an individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee shall be reported.

c. **Change in Cleared Employee Status.** The following shall be reported:

1. Death.
2. Change in name.
3. Termination of Employment.
4. Change in marital status.
5. Change in citizenship.
6. When the access to classified information in the future has been reasonable foreclosed.

d. **Representative of a Foreign Interest.** Any cleared employee, who becomes a representative of a foreign interest (RFI) or whose status as an RFI is materially changed shall be reported.

e. **Citizenship by Naturalization.**

f. **Employees Desiring Not to Perform on Classified Work.**

g. **Standard Form (SF) 312.** Refusal by an employee to execute the "Classified Information nondisclosure Agreement" (SF 312).

h. **Changed Conditions Affecting the Facility Clearance.**

1. Any change of ownership.
2. Any change of operating name or address of the company.
3. Any change to the information previously submitted for key management personnel.
4. Action to terminate business or operations for any reason.

5. Any material change concerning the information previously reported by the contractor concerning foreign ownership, control or influence (FOCI). A new CSA –designated form regarding FOCI shall also be executed every 5 years.

i. **Change in Storage Capability.**

j. **Inability to Safeguard Classified Material.**

k. **Security Equipment Vulnerabilities.**

l. **Unauthorized Receipt of Classified material.**

m. **Employee Information in Compromise Cases.**

n. **Foreign Classified Contracts.**

o. **Foreign Travel**

1. All Foreign travel must be reported to the Security Department prior to actual travel. A defensive travel briefing will be administered and a briefing form signed by employee. This briefing will be retained for the life of the program.
2. Travel by program briefed individuals into or through countries determined by the CSA as high risk areas, should not be undertaken without prior notification to the Security Manager.

p. **Litigation.** Litigation or public proceedings which may involve a SAP will be reported to the Security Manager.

q. **Arms control treaty visits.**

r. **Security violations and improper handling of classified information.**

1. A security violation is any incident that involves the loss, compromise, or suspected compromise of classified information. Security violations will be immediately reported within 24 hours to the PSO.

2. A security infraction is any other incident that is not in the best interest of security that does not involve a loss, compromise or suspected compromise of classified information. Security infractions will be documented and made available for review by the PSO during visits.

3. Inadvertent Disclosure is the involuntary, unauthorized access to classified SAP information by an individual without SAP access authorization. Personnel exposed to unauthorized SAP information must be interviewed to determine the extent of exposure and will complete an inadvertent disclosure oath. Refusal to sign inadvertent disclosure oath will be reported by the CPSO to the PSO.

1-303. Reports of Loss, Compromise, or Suspected Compromise. Any loss, compromise or suspected compromise of classified information, foreign or domestic, shall be reported. Classified material that cannot be located within a reasonable period of time shall be presumed to be lost until an investigation determines otherwise.

a. **Preliminary Inquiry.** Immediately on report of loss, compromise, or suspected compromise of classified information, a preliminary inquiry is done to ascertain all of the circumstances surrounding the reported loss, compromise, or suspected compromise.

b. **Initial Report.** If it is confirmed that a loss, compromise, or suspected compromise of any classified information occurred, an initial report of the incident shall be completed.

c. **Final Report.** When the investigation has been completed, a final report shall be submitted.

1-304. Individual Culpability Reports. The following are guidelines for disciplinary actions as might be necessary to correct security deficiencies.

a. **Minor Security Violations.** (within a 12 month period) Resulting from oversight or unintentional failure to comply with security regulations or requirements and which does not result in the compromise or suspected compromise of classified information.

1. **First minor** violation, individual will be counseled by Project Manager/Supervisor, rebriefed as to their security responsibilities and given a documented verbal reprimand.
2. **Second minor** violation, individual will be counseled by the Group Vice-President, rebriefed by the Security Manager, given a written reprimand and placed on probation.
3. **Third minor** violation, individual will be counseled by the Group Vice-President, rebriefed by the Security Manager, given a written reprimand, suspended without pay for up to three days and placed on probation.

4. **Fourth minor** violation, individual will be terminated.

b. **Major Security Violations.** (within a 12 month period) Willful disregard of security regulations, or the failure through negligence to comply with any security regulation or requirement and which results in the compromise or suspected compromise of classified information.

1. **First major** violation, individual will be counseled by the Group Vice-President, rebriefed by the Security Manager, given a written reprimand and placed on probation.
2. **Second major** violation, individual will be counseled by the Group Vice-President, Security manager, and suspended without pay for three days.
3. **Third major** violation, individual will be terminated.

c. Supervisors are not required to go through all the steps of the disciplinary process. Discipline may begin at any point depending on the seriousness of the employee's actions. If an employee's actions constitute a major violation, that employee may be dismissed for cause.

d. Additionally, in disciplinary situations involving combinations of minor/major infractions and/or other varying types of previous disciplinary actions, the supervisor may also initiate actions in accordance with the above paragraph.

e. Written accounts of security violations will be maintained in the employee's permanent personnel security file for a period of twelve months from the date of the incident.

CHAPTER 2. SECURITY CLEARANCES

Section 1. Facility Clearances. Facility clearances will be maintained in accordance with Chapter 2, Section 1 of the NISPOM and Chapter 2, Section 1 of the NISPOMSUP.

Section 2. Personnel Clearances

2-200. Policy. All employees within Las Vegas Operations of EG&G Technical Services are required to have a Department of Defense (DoD) security clearance and may require a special grant of access to work at certain locations and/or to be assigned to certain programs. All security clearances will be processed according to Section 2, Chapter 2 of the NISPOM. Employees must be granted the required clearance and access (if required) within 365 days of their date of hire (or subsequent date of selection for a position requiring a higher level of clearance). Furthermore, employees having been granted clearance/access will be expected to maintain these requirements throughout their term of employment. Employees failing to do so are subject to dismissal.

2-201. Applicability. This chapter applies to all employees of EG&G Technical Services.

2-202. Definitions.

a. **Top Secret Clearance.** Permits an individual to have access, on a need-to-know basis, to Top Secret, Secret, or Confidential information as required in the performance of duties. Top Secret clearances are based on Single Scope Background Investigations (SSBI) conducted by the Defense Investigative Service (DIS).

b. **Secret Clearance.** Permits an individual to have access, on a need-to-know basis, to Secret or Confidential information as required in the performance of duties. Secret clearances may be based on an SSBI; however normally, Secret clearances are based upon National Agency Checks (NAC).

c. **Confidential Clearance.** Permits an individual to have access, on a need-to-know basis, to Confidential information as required in the performance of duties.

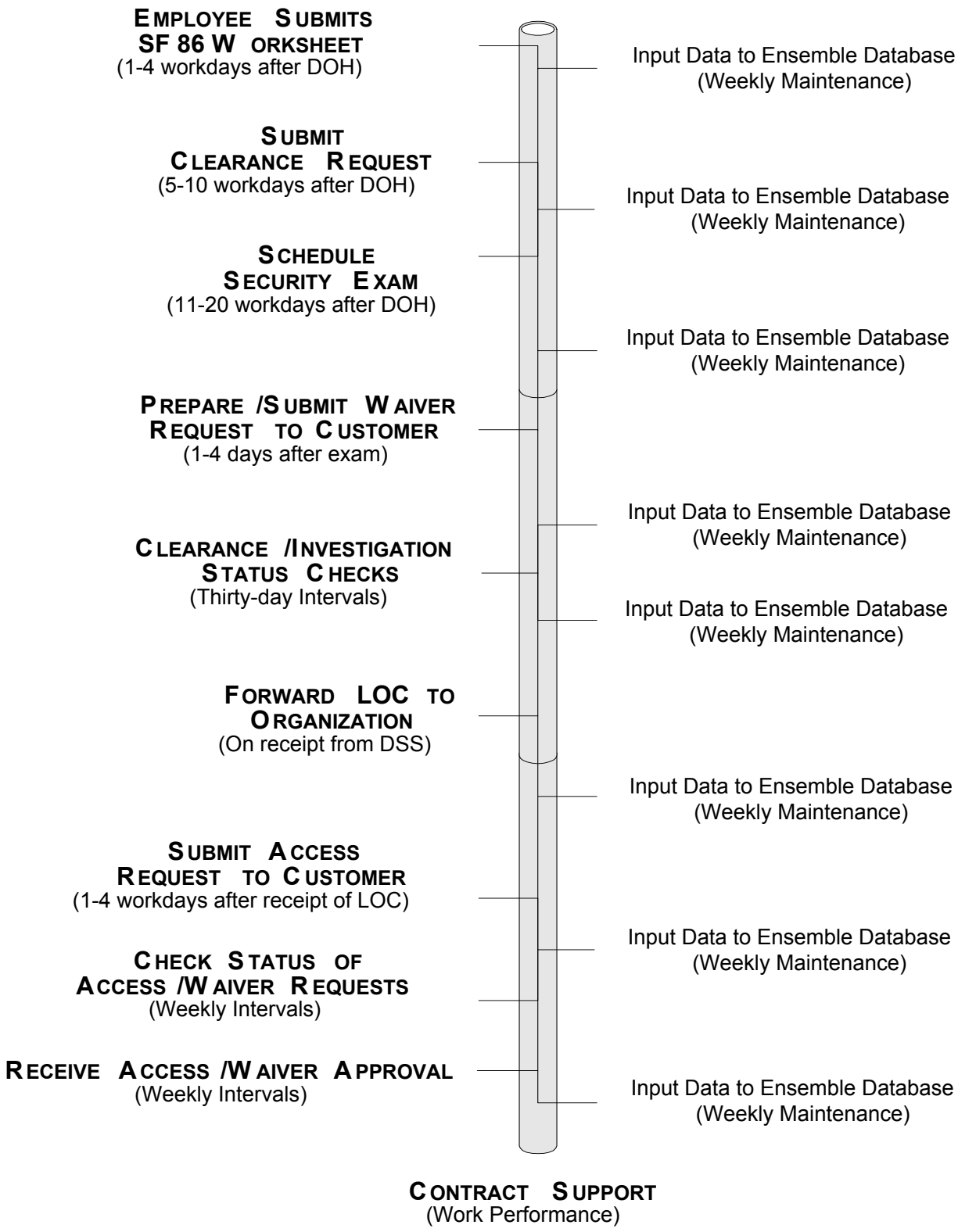
d. **Q-Clearance.** Permits an individual to have access, on a need-to-know basis, to Top Secret, Secret, and Confidential Restricted Data, Formerly Restricted Data, National Security Information, or special nuclear material in Category I or II as required in the performance of duties.

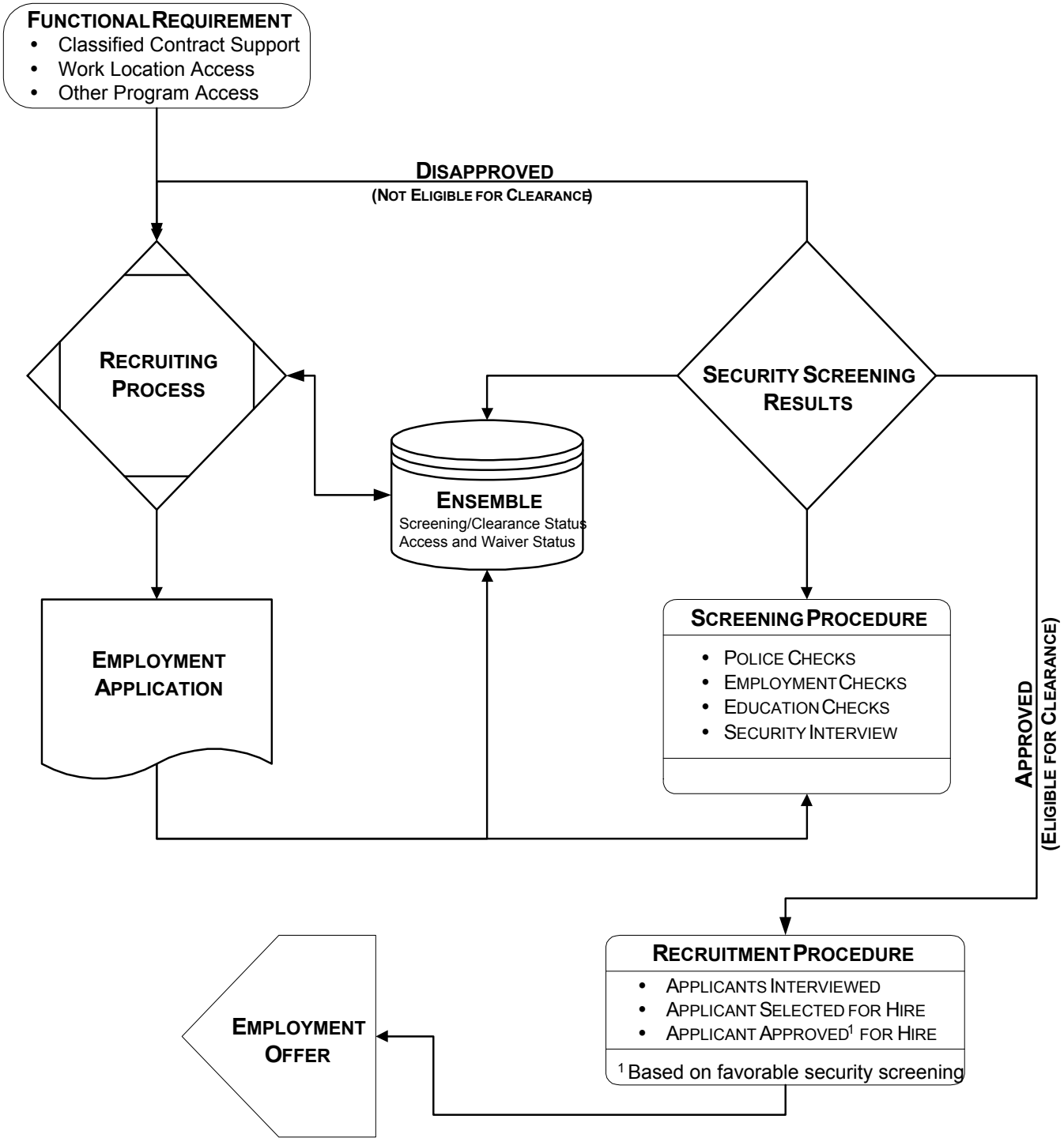
e. **Single Scope Background Investigation.** A personal security investigation conducted by various government agencies. An SSBI covers a ten-year period and consists of a NAC, subject interview, verification of birth, citizenship, education, and employment. It also includes references, credit, public records, and neighborhood and local agency checks.

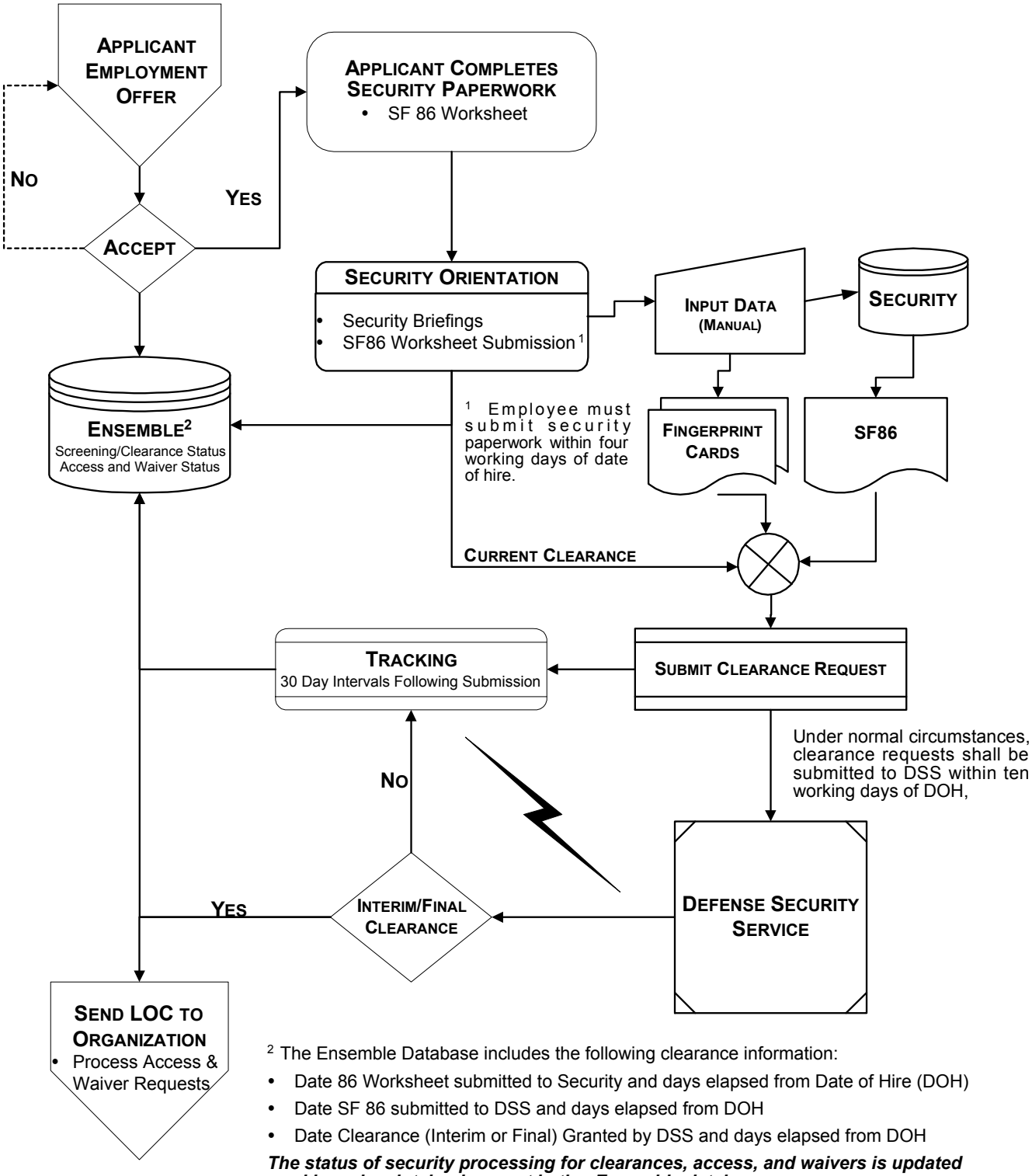
h. **Periodic Reinvestigation.** A personal security investigation to update previously completed investigations. Periodic reinvestigations normally cover the preceding five-year period and consist of a personal interview and all components of the investigation being updated. Such reinvestigations are required by personnel employed in certain categories of duties or who have access to certain categories of information.

i. **Special Access.** Access controls beyond those normally provided by a security clearance for access to Confidential, Secret, or Top Secret information. Such access generally requires separate and specific access determinations, additional restrictions for the dissemination of classified information, and the maintenance of special lists of personnel having a need-to-know.

2-203. The following four pages are the procedures for obtaining a security clearance and gaining site access:


DATE OF HIRE (DOH)
EMPLOYEE SUBMITS SF 86 WORKSHEET
(1-4 workdays after DOH)
Input Data to Ensemble Database
(Weekly Maintenance)
SUBMIT CLEARANCE REQUEST
(5-10 workdays after DOH)
Input Data to Ensemble Database
(Weekly Maintenance)
SCHEDULE SECURITY EXAM
(11-20 workdays after DOH)
Input Data to Ensemble Database
(Weekly Maintenance)
PREPARE /SUBMIT WAIVER REQUEST TO CUSTOMER
(1-4 days after exam)
Input Data to Ensemble Database
(Weekly Maintenance)
CLEARANCE /INVESTIGATION STATUS CHECKS
(Thirty-day Intervals)
Input Data to Ensemble Database
(Weekly Maintenance)
FORWARD LOC TO ORGANIZATION
(On receipt from DSS)
Input Data to Ensemble Database
(Weekly Maintenance)
SUBMIT ACCESS REQUEST TO CUSTOMER
(1-4 workdays after receipt of LOC)
Input Data to Ensemble Database
(Weekly Maintenance)
CHECK STATUS OF ACCESS /WAIVER REQUESTS
(Weekly Intervals)
RECEIVE ACCESS /WAIVER APPROVAL
(Weekly Intervals)
Input Data to Ensemble Database
(Weekly Maintenance)
CONTRACT SUPPORT
(Work Performance)

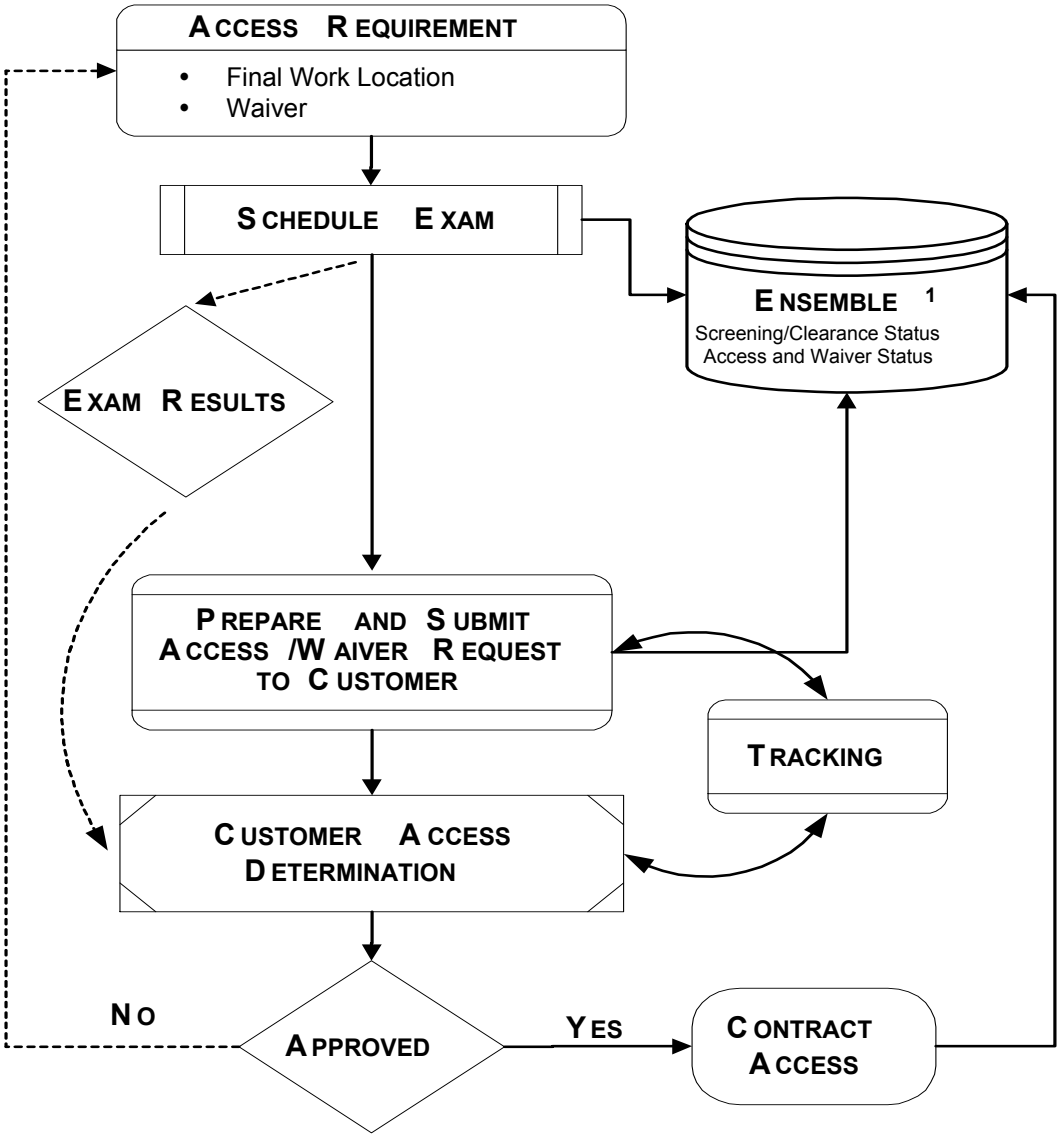

FUNCTIONAL REQUIREMENT
• Classified Contract Support
• Work Location Access
• Other Program Access
DISAPPROVED
(NOT ELIGIBLE FOR CLEARANCE)
RECRUITING PROCESS
SECURITY SCREENING RESULTS
ENSEMBLE
Screening/Clearance Status
Access and Waiver Status
EMPLOYMENT APPLICATION
SCREENING PROCEDURE
• POLICE CHECKS
• EMPLOYMENT CHECKS
• EDUCATION CHECKS
• SECURITY INTERVIEW
APPROVED
(ELIGIBLE FOR CLEARANCE)
RECRUITMENT PROCEDURE
• APPLICANTS INTERVIEWED
• APPLICANT SELECTED FOR HIRE
• APPLICANT APPROVED[1] FOR HIRE
[1] Based on favorable security screening
EMPLOYMENT OFFER



[2] The Ensemble Database includes the following clearance information:

- Date 86 Worksheet submitted to Security and days elapsed from Date of Hire (DOH)
- Date SF 86 submitted to DSS and days elapsed from DOH
- Date Clearance (Interim or Final) Granted by DSS and days elapsed from DOH

The status of security processing for clearances, access, and waivers is updated weekly and maintained current in the Ensemble database.



[1] The Ensemble Database includes the following clearance information:

- Date 86 Worksheet submitted to Security and days elapsed from Date of Hire (DOH)
- Date SF 86 submitted to DSS and days elapsed from DOH
- Date Clearance (Interim or Final) Granted by DSS and days elapsed from DOH

The status of security processing for clearances, access, and waivers is updated weekly and maintained current in the Ensemble database.

2-204. SAP Accessing Requirements.

a. The employee must have a valid need to know (NTK) and will materially and directly contribute to the program.

b. Employee must possess a minimum of a current, final Secret security clearance or meet the investigative criteria required for the level of access. If the persons periodic reinvestigation (PR) is outside the five year scope the individual will immediately processed for a single scope background investigation.

c. EG&G will nominate the individual and provide a description of the NTK justification. EG&G CPM with concur with the nomination and verify Program contribution by signature on the Program Access Request (PAR). The FSO will complete the PAR and review it for accuracy ensuring all required signatures are present. The PAR will be submitted to the PSO for evaluation and review. The PSO with notify EG&G of access or denial.

d. Subcontractors may submit the PAR package to the prime. The prime will review and concur on the PAR and forward the PAR to the PSO.

e. SCI access will follow guidelines established in DCID 1/14.

f. SAP access will follow guidelines established by the Security Policy Board with clarifications listed in Chapter 2, Section 2-201-h of the NISPOMSUP.

g. Briefings: SAP Briefings will be conducted by the PSO upon approval.

h. PRs will be submitted on employees every five years. SAP points of contact (POCs), Program Names or other program identifiers will not be put on form DD1879 unless approved by PSO.

2-205. Consultants. Consultants will be processed for security clearance the same as regular EG&G employees. A consultant to a SAP activity must have the appropriate personnel security clearance on file and will be approved for Program Access by the GPM and PSO. The consultant will perform classified work at an approved SAPF in accordance with form DD 254. EG&G will submit to the PSO a copy of their Statement of Work detailing what specific task he/she will be performing. Once consultant status is approved the consultant PAR package, which will also include an executed consultant agreement, will be submitted to the PSO for approval. Any change in the consultant status must be reported immediately to the GPM and PSO.

Section 3. Foreign Ownership, Control, or Influence (FOCI). Not applicable at this time.

CHAPTER 3. SECURITY TRAINING AND BRIEFINGS

Section 1. Security Briefings/Debriefings. All briefings addressed in this section will be administered by the FSO or a designated representative.

3-100. General. To provide a comprehensive security education program as required in the NISPOM and NISPOMSUP through briefings and training to all EG&G employees granted access to classified material.

Responsibilities:

a. FSO: The FSO or his designated representative will be responsible for administering the overall security education program.

b. Security Education Representatives (SERs) will be responsible for providing refresher and security awareness training to all company employees at remote work locations.

Procedures:

a. All initial security briefings will be provided by the FSO or designated representative during new employee in-processing.

b. All refresher and security awareness training will be provided by the SERs at the remote work locations and the FSO at the downtown locations.

c. All SAP briefings will be provided by the Customer through the PSO or his designated representative at the appropriate time.

d. All security debriefings will be provided by either the Customer or EG&G FSO whenever program access is no longer required or employee terminates.

e. Foreign travel briefings will be provided by either the Customer at the remote work locations or the company FSO at the downtown locations.

3-101. Training Materials. All training materials will be provided by the Security Department to the FSO and SERs. SAP training material will be provided by the Customer.

3-102. FSO Training. EG&G FSO will be required to complete the FSO Management Course within one year from appointment to the FSO position.

3-103. Government-Provided Briefing. The CS is responsible for providing initial security briefings to the FSO, and for ensuring that other briefings required for special categories of information are provided.

3-104. Classified Information Nondisclosure Agreement (SF 312). The SF 312 is an agreement between the United States and an individual who is cleared for access to classified information. An employee issued an initial PCL must execute a SF 312 prior to being granted access to classified information. If the employee refuses to execute the SF 312, the company shall deny the employee access to classified information and submit a report to the CSA. The SF 312 shall be signed and dated by the employee and witnessed. The employee and witness' signatures must bear the same date.

3-105. Initial Security Briefings. Prior to being granted access to classified information, an employee shall receive an initial security briefing that includes the following:

a. A Threat Awareness Briefing.

b. A Defensive Security Briefing.

c. An overview of the security classification system.

d. Employee reporting obligations and requirements.

e. Security procedures and duties applicable to the employee's job.

3-106. Refresher Training. Refresher training will be provided at least annually and will reinforce the information provided during the initial security briefings including both NISPOM and SAP requirements.

3-107. Debriefings. The company FSO or Customer Representative will debrief cleared employees at the time of termination of employment (discharge, resignation, or retirement); when an employee's PCL is terminated, suspended, or revoked; and upon termination of the FCL. Topics will include:

a. Purpose of the debriefing.

b. The serious nature of the subject matter requiring protection.

c. The need for caution and discretion.

d. Advise on appropriate travel restrictions.

Section 2. SAP Security Training.

3-200. General. Every SAP will have a Security Training and Briefing Program. In addition to the NISPOM baseline training and briefing provided employees by the company those employees access to SAP information will also receive the following types of SAP briefings:

a. **Indoctrination briefing addressing the following topics:**

1. Security requirements unique to SAPs;
2. Protection of classified relationships;
3. Operations Security (OPSEC);
4. Use of nicknames and code words;
5. Use of special transmissions methods;
6. Special test-range security procedures;
7. Procedures for Unacknowledged SAP security;
8. Special procedures to report fraud, waste, and abuse;
9. Computer security education to include operational procedures, threats, and vulnerabilities;
10. Writing unclassified personnel appraisals and reviews;
11. Third Party Introductions.

b. **Unacknowledged SAPs briefing with special emphasis on:**

1. Why the SAP is Unacknowledged;
2. Classification of the SAP;
3. Approved communications system;
4. Approved Transmission systems;
5. Visit procedures;
6. Specific program guidance.

c. **Refresher Briefings will be provided annually and will include the following topics:**

1. Review of Program-unique security directives or guidelines;
2. Review of those elements contained in the original SF 312;
3. Foreign intelligence techniques and threat reporting;
4. Discussing program information over unsecured telephones and use of STU IIIs. Brief STU IIIs operations annually;
5. Information concerning actual or potential terrorism, terrorist groups, espionage, or sabotage of any U.S. facility, activity, person, or resource;
6. Adverse affects to national security resulting from unauthorized disclosure;
7. Derivative classification and marking requirements;

8. Adverse reporting;
9. Reporting FWA through SAP Channels;
10. Program vulnerabilities, program threat, and OPSEC;
11. Computer security to include operating procedures, audit trails, logs, forms, receipts, media protection, use of system copyright laws, and licensing agreements;
12. Common security deficiencies discovered during recent self reviews;
13. Reporting of personal status changes;

d. Foreign Travel Briefing is provided to all accessed personnel annually or before travel, whichever is earlier. Briefing will include both general and country specific information and threat advisories. Also include foreign intelligence techniques, terrorists activities, civil situations, or other hazards to personnel safety. In addition reporting of foreign contacts must be discussed. Individuals accessed to multiple SAPs need only attend one foreign travel briefing.

e. Specialized Training Briefing is given periodically throughout the time the employee is accessed to the SAP. This briefing is usually provided by the PSM or the FSO when special events are scheduled. Topics include specific items of interests, security inspection results, new test, or change in program status. Should also include a defensive briefing on elicitation techniques used by FIS to persons attending international conferences and symposia. Specialized training will also include courier briefing to SAP personnel performing courier duty.

f. Termination Debriefing. Persons briefed to SAPs will be debriefed by the company FSO or his designee using the Customer Debriefing Form. The individual must sign the debriefing form and witnessed by the FSO with appropriate signatures. The employee will be briefed in the following:

1. Remind the employee of his/her continuing obligations agreed to in the SAP NDA.
2. Remind the employee that the NDA is a legal contract between the individual and the U.S. Government.
3. Advise the employee that all classified information to include Program information is now and forever the property of the U.S. Government.
4. Remind individual of the penalties for espionage and unauthorized disclosure as contained in Titles 18 and 50 of the U.S. Code.
5. Remind employee of his/her obligation not to discuss, publish, or otherwise reveal information about the Program. The appearance of Program information in the public domain does not constitute a de facto release from the continuing secrecy agreement.
6. Advise that any future questions or concerns regarding the Program will be directed to the PSO or FSO. The employee will be given a telephone number for the FSO or the PSO.

7. Advise the employee that each provision of the agreement is severable (i.e., if one provision is declared unenforceable, all others remain in force.)
8. Emphasize that even though an individual signs a Debriefing Acknowledgement Statement, he/she is never released from the original NDA/secrecy agreement unless specified in writing.

g. If the employee refuses to execute a debriefing form, administer an oral debriefing in the presence of a witness and annotate the debriefing form: "ORAL DEBRIEFING CONDUCTED; EMPLOYEE REFUSED TO SIGN". The briefer and the witness sign beneath the statement attesting to this action. Immediately report this action to the PSO.

CHAPTER 4. CLASSIFICATION AND MARKING

Section 1. Classification

4-100. General. Derivative classification decisions are based on the guidance provided by the Contract Security Classification Specification that is issued with each classified contract.

4-101. Derivative Classification Responsibilities. **A**ll employees authorized to perform derivative classification actions are sufficiently trained and possess, or have ready access to, the pertinent classification guides and/or guidance necessary to fulfill these important actions.

a. Individual employees who copy or extract classified information from another document, or who reproduce or translate an entire document, shall be responsible for marking the new document or copy with the same classification markings as applied to the information or document from which the new document or copy was prepared.

4-102. Downgrading or Declassifying Classified Information. Information is downgraded or declassified based on the guidance provided in the Contract Security Classification Specification upon formal notification or as shown on the material.

4-103. DD Form 254 Requirements.

a. A DD Form 254, DoD Contract Security Classification Specification, for each contract, subcontractor, or consultant will be prepared. The DD 254 will be used to transmit the Program Security Guide (PSCG) and other documents containing security classification guidance.

b. A current listing of the location of containers, rooms, and completely dedicated buildings that contain SAP materials and are carved out from DSS cognizance is kept. This information is provided to the PSO.

c. The PSO provides detailed guidance pertaining to DD Forms 254 on classification, release to the DSS, carve-out status, etc. This guidance is based on the specific PSCG.

Section 2. Marking Requirements

4-200. General. Classified information and material are marked to clearly convey to the holder the level of classification assigned, the portions that contain or reveal classified information, the period of time protection is required, and any other notations required for protection of the information or material.

4-201. Identification Markings. All classified material shall be marked to show the name and address of the facility responsible for its preparation, and the date of preparation. These markings are required on the face of all classified documents. The PSO may specify additional markings to be applied to SAP working papers based on the sensitivity and criticality of the Program, when approved by the CSA.

a. All program-classified documents, media, and materials will contain the following markings on the top and bottom of each page:

SECRET/CODEWORD or **NICKNAME** or **SPECIAL ACCESS REQUIRED**

b. All derivitave program-classified documents, media, and materials will contain the following markings:

DERIVED FROM: (source document or classification guide)
DECLASSIFY ON: (date, event or OADR)

c. The following are originating authority choices for determining the declassification date (NISPOMSUP Chapter 4, Section 2):

1. Ten years from the date of the original decision (not the date the document was originated).

2. Extension of a 10 year classification.

3. Name of the person (a designated original classification authority) signing the guide or document.

4. Declassify on: Specific Date or Event. (See NISPOMSUP Chapter 4, Section 2.

4-202. Identification Markings. All classified material will be marked to show:

a. The name and address of the facility responsible for its preparation.

b. The date of preparation.

c. These markings are required on the face of all classified material.

d. Unless the classification is based on a compilation of information, portion markings are required for each document. Classified as well as unclassified paragraphs will be identified. SAP paragraphs will be marked with the classification abbreviations.

e. When marking documents containing a specific SAP's information, the following paragraph or portion markings will be used:

1. The classification of the paragraph: CONFIDENTIAL, SECRET, or TOP SECRET.

2. An appropriate program identifier.

4-203. Cover Sheets. Cover sheets will be applied to SAP documents when the documents are created or distributed. *NOTE: CODE WORDS WILL NOT BE PRINTED ON THE COVER SHEETS.* The unclassified nickname, diagraph, or trigraph may be used.

4-204. Overall Markings. The highest level of classification will be conspicuously marked or stamped on a documents, or any copy or reproduction thereof, on the top and bottom of the front cover (if any), the title page (if any), the first page, and on the outside of the back cover (if any). If the document does not have a back cover, the outside of the back or last page, which may serve as a cover, may also be marked at the top and bottom with the overall classification of the document.

a. Markings shall be stamped, printed, etched, written, engraved, painted or affixed using a tag, sticker, decal or similar means, on material other than documents and on containers for material, if possible.

b. If marking the material or container is not practical, written notification of the markings shall be furnished to recipients.

4-205. Page Markings. Interior pages of classified documents shall be conspicuously marked or stamped at the top and bottom with the highest classification of the information appearing thereon, or the designation UNCLASSIFIED, if all the information on the page is unclassified. Alternatively, the overall classification of the document may be conspicuously marked or stamped at the top and bottom of each interior page, when necessary to achieve production efficiency, and the particular information to which classification is assigned is adequately identified by portion markings.

4-206. Component Markings. Each major component shall be marked as a separate document in case each major component is used separately. Examples include:

a. Each annex, appendix, or similar component of a plan, program or project description.

b. Attachment and appendices to a letter.

c. Each major part of a report.

4-207. Portion Markings. Each section, part, paragraph, or similar portion of a classified document will be marked to show the highest level of its classification, or that the portion is unclassified. Portions will be marked so as to eliminate doubt as to which portion contains or reveals classified information.

a. Portions or paragraphs shall be considered a distinct section or subdivision of a chapter, letter, or document dealing with a particular point or idea, which begins on a new line and is often indented.

b. Classification levels for portions of a document shall be shown by a classification symbol placed immediately following that portion's letter or number, or if no letter or number, immediately before the beginning of the portion. Parenthetical symbols to be used are:

1. (TS) for TOP SECRET
2. (S) for SECRET
3. (C) for CONFIDENTIAL
4. (U) for UNCLASSIFIED

c. Illustrations, photographs, figures, graphs, drawings, charts, or similar items contained in documents will be marked clearly to show their classified or unclassified status. These classification markings shall not be abbreviated and shall be prominent and placed within or touching or near to such item. Captions of such portions shall be marked on the basis of their content alone by placing the symbol (TS), (S), (C), and (U) immediately preceding the caption.

1. Should elements of a portion or paragraph require separate levels of classification and separation would impair continuity or context, use the highest level of classification for that portion or paragraph.

4-208. Subject and Title Markings. Unclassified subjects and titles shall be selected for classified documents, if possible. An unclassified subject or title shall be marked with a (U) placed immediately following and to the right of the item. A classified subject or title shall be marked with the appropriate symbol (TS), (S), or (C) placed immediately following and to the right of the item.

4-209. Marking Special Types of Material.

a. Files, folders, binders, envelopes and other items containing classified documents, when not in secure storage, shall be conspicuously marked with the highest classification of any classified item included therein. Cover sheets may be used for this purpose.

b. Electronically transmitted messages shall be marked in the same manner required for other documents.

4-210. Marking Transmittal Documents. A transmittal document shall be marked with the highest level of classified information contained therein and with an appropriate notation to indicate its classification when the enclosures are removed.

4-211. Marking Compilations.

a. **Documents.** When classification is required to protect a compilation of information, the overall classification assigned to the document shall be conspicuously marked or stamped at the top and bottom of each page and on the outside of the front and back covers, if any. The reason for classifying the compilation shall be stated at an appropriate location at or near the beginning of the document.

b. **Portions of a Document.** If a classified document contains certain portions that are unclassified when standing alone, but classified information will be revealed when they are combined or associated, those portions shall be marked as unclassified, the page shall be marked with the highest classification of any information on the page, and a statement shall be added to the page, or to the document, to explain the classification of the combination or association to the holder.

4-212. Marking Training Material. Unclassified documents or material that are created to simulate or demonstrate classified documents or material shall be clearly marked to indicate the actual UNCLASSIFIED status of the information.

4-213. Marking Downgraded or Declassified Material.

a. **Automatic Downgrading or Declassification Actions.** All old classification markings shall be cancelled and the new markings substituted, whenever practical. At a minimum, the outside of the front cover (if any), the title page (if any), the first page, and the outside of the back cover (if any), shall reflect the new classification markings, or the designation UNCLASSIFIED. Other material shall be remarked by the most practical method for the type of material involved to ensure that it is clear to the holder what level of classification is assigned to the material.

b. **Other than Automatic Downgrading or Declassification Actions.** When we are notified of downgrading or declassification actions that are contrary to the markings shown on the material, the material shall be remarked to indicate the change in the same manner as stated in 4-212.

4-214. Upgrading Action. When we receive notice to upgrade material to a higher level, the new markings shall be immediately entered on the material in accordance with the notice to upgrade, and all the superseded markings shall be obliterated. The authority for, and the date of, the upgrading action shall be entered on the material.

4-215. Miscellaneous Actions. If classified material is inadvertently distributed outside the facility without the proper classification assigned to it, or without any markings to identify the material as classified the following actions will be taken as appropriate.

a. Determine whether all holders of the material are cleared and are authorized access to it.

b. Determine whether control of the material has been lost.

c. If recipients are cleared for access to the material, promptly provide written notice to all holders of the proper classification to be assigned. If control of the material has been lost, if all copies cannot be accounted for, or if unauthorized personnel have had access to it, report the compromise to the CSA.

d. In the case of classified material being upgraded, written notice shall not be classified unless the notice contains additional information warranting classification. In the case of material which was inadvertently released as UNCLASSIFIED, written notice shall be classified CONFIDENTIAL, unless it contains additional information warranting a higher classification. The notice shall cite the applicable Contract Security Classification Specification or other classification guide on the "Derived From" line and be marked with an appropriate declassification instruction.

4-216. Engineer's Notebook. An engineer's notebook is a working record of continually changing Program technical data. It should not include drafts of correspondence, reports, or other materials. The outer cover and first page will be marked with the highest classification level contained in the notebook. Portion marking or numbering is not required. Other requirements pertaining to these notebooks may be imposed by the PSO.

4-217. Warning Notices. Generally, Program classified marking and transmissions requirements will follow the NISPOMSUP. Transmission of Program or Program-related material will be determined by the PSO. Besides the classification markings, inner containers will be marked:

"TO BE OPENED ONLY BY:"

followed by the name of the individual to whom the material is sent. A receipt may be required. The following markings will be applied on the bottom center of the fron of the inner container:

WARNING: THIS PACKAGE CONTAINS CLASSIFIED U.S. GOVERNMENT INFORMATION. TRANSMISSION OR REVELATION OF THIS INFORMATION IN ANY MANNER TO AN UNAUTHORIZED PERSON IS PROHIBITED BY TITLE 18, U.S. CODE, SECTION 798 (OR TITLE 42, SECTION XX FOR RD OR FRD MATERIAL). IF FOUND, PLEASE DO NOT OPEN. "CALL COLLECT" THE FOLLOWING NUMBERS: 702-361-1660 X 1044 DURING WORKING HOURS OR 702 736-3740 AFTER WORKING HOURS.

The protective marking Handle Via Special Access Channels Only (HVSACO) may be imposed by the PSO to identify information which must remain in SAP controlled protective channels.

CHAPTER 5. SAFEGUARDING CLASSIFIED INFORMATION

Section 1. General Safeguarding Requirements

5-100. General. The extent of protection afforded classified information is sufficient to reasonably foreclose the possibility of its loss or compromise. Classified and unclassified sensitive SAP material must be stored in SAP CSA approved facilities only. Any deviations must have prior approval of the SAP CS or designee.

5-101. Safeguarding Oral Discussions. All cleared employees are made aware of the prohibition against discussing classified information over unsecured telephones, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

5-102. End of Day Security Checks.

a. Security checks will be performed at the end of each work day to ensure that classified material not under surveillance has been properly stored.

b. Each project area will conduct an end of day Security check to ensure that classified material not under surveillance has been properly stored.

5-103. Perimeter Controls. An Access Control Officer will be on duty in the front lobby during business hours. Security camera monitors are located at the ACO desk.

a. All persons who enter or exit the facility are subject to an inspection of their personal effects. Random searches are conducted and logged.

b. The ACO conducts an end of day check of the facility before securing the facility.

5-104. Emergency Procedures. In the event of an incident or circumstances which would reduce, restrict or inhibit EG&G Technical Services ability or capability to protect/store program material, the following procedures will be initiated:

a. The FSO will assign two or more program accessed personnel to maintain constant custody of all program related material until EG&G Technical Services ability/capability to protect or store such information/material is restored, or:

b. All program related material is inventoried, packaged and dispatched via courier procedures to another controlled facility for storage.

Section 2. Control and Accountability

5-200. General. All classified information is controlled under Document Control.

5-201. External Receipt and Dispatch Records. A Receipt for Material will accompany all classified information when dispatched. This receipt will include:

a. Date of Material
b. Date of Receipt
c. Classification
d. Unclassified description of classified information

5-202. Accountability for TOP SECRET.

a. The Document Control Coordinator is designated the TOP SECRET control officer to receive, transmit, and maintain access and accountability records for TOP SECRET information.

b. The transmittal of TOP SECRET information is covered by a continuous receipt system both within and outside the facility.

c. TOP SECRET material is logged and numbered. The copy number is placed on TOP SECRET documents and on all associated transaction documents. Top Secret working papers will be logged and numbered or destroyed within 30 calendar days of origin.

d. A disclosure (access record) is maintained for each TOP SECRET document. This record is filed with the document or in the safe with computer equipment.

5-203. COMSEC. All COMSEC material will be accounted for in accordance with published COMSEC guidelines.

5-204. Vendor Software. Vendor software shall be accounted for in accordance with NISPOMSUP.

5-205. SECRET/SAR. Secret/Sar material will be fully accounted for.

5-206. Receiving Classified Material. All classified material will be delivered unopened to Document Control. NOTE: All Registered Mail, Certified Mail, or U.S. Express Mail (Signature Service) will be treated as classified and will not be opened by any other person than Document Control Coordinator, FSO, or a Security staff member.

a. Each package shall be examined for any evidence of tampering and the classified contents shall be checked against the receipt. Discrepancies in the contents of a package or absence of a receipt shall be reported immediately to the FSO and the sender. If the shipment is in order, the receipt shall be signed and returned to the sender. For purposes of identification, the name of the employee signing the receipt shall also be printed or typed.

5-207. Generation of Classified Material.

a. A record of classified material produced by EG&G Technical Services shall be made when the material is: (1) Completed as a finished document; (2) Retained for more than 30 days after creation, regardless of the stage of development; or (3) Transmitted outside the facility.

b. Classified working papers generated in the preparation of a finished document shall be: (1) Dated when created; (2) Marked with its overall classification, and with the annotation, "WORKING PAPERS;" and (3) Destroyed when no longer needed.

b. Working papers shall be marked in the same manner prescribed for a finished document at the same classification level when: (1) Transmitted outside the facility; or (2) Retained for more than 180 days from creation.

5-208. Annual Inventory. A semi-annual inventory by Security Personnel is done between annual Security Reviews by the Customer.

5-209. Retention Requirements for Accountability Logs.

5-210. TOP SECRET/SAR Working Papers. Top Secret/Sar working papers are handled and accounted for as a document upon creation.

5-211. SECRET/SAR Working Papers. Secret/Sar working papers shall be properly classified and marked and protected in an approved SAPF. Secret/Sar working papers shall be entered into the accountability system or destroyed within 30 calendar days from the date of origin.

5-212. TOP SECRET and SECRET/SAR Working Notebooks. A document control number is assigned to the notebook. Pages are pre-numbered individually. The outer cover is marked with the highest anticipated classification. Entries are dated when they are created. Each page is marked with the highest classification.

Section 3. Storage and Storage Equipment

5-300. General. This section describes the physical protection of classified material in the custody of EG&G Technical Services.

5-301. TOP SECRET STORAGE. TOP SECRET material shall be stored in a GSA-approved security container, an approved vault or an approved Closed Area. Safe and cabinet security records shall be kept on all safes and all openings and closings shall be recorded. The Access Control Officer (ACO) will initial the security record when on rounds at the end of the workday

check. Supplemental protection is provided by way of Alarm system and Access Control Officer. Approved vaults at the 821 Grier Drive facility include:

a. ROOM 103
b. ROOM 104
c. ROOM 105
d ROOM 106 (SCIF)

5-302. SECRET Storage. SECRET material shall be stored in the same manner as TOP SECRET material or in approved steel file cabinet with metal lock bar.

5-303. CONFIDENTIAL Storage. CONFIDENTIAL material shall be stored in the same manner as TOP SECRET or SECRET material.

5-304. Closed Areas. Closed areas in the 821 Grier Drive facility include:

a. ROOM 110
b. ROOM 204
c. ROOM 213
d. ROOM 214
e. ROOM 215
f. ROOM 216
g. ROOM 218

Access to these areas is controlled by a Card Reader System and MDI Alarm System. In addition there is an Access Control Officer at the front entrance during working hours.

5-305. Protection of Combinations to Security Containers, Cabinets, Vaults and Closed Areas.

a. A record of the names of persons having knowledge of the combination shall be maintained in the Project area safe.

b. Security containers, vaults, cabinets, and other authorized storage containers shall be kept locked when not under the direct supervision of an authorized person entrusted with the contents.

c. The combination shall be safeguarded in accordance with the highest classification of the material authorized for storage in the container.

d. A record of the combination shall be marked with the highest classification of material authorized for storage in the container.

5-306. Changing Combinations. Combinations shall be changed by a person authorized access to the contents of the container, or by the FS0 or his or her designee. Combinations shall be changed as follows:

a. The initial use of an approved container or lock for the protection of classified material.

b. The termination of employment of any person having knowledge of the combination, or when the clearance granted to any such person has been withdrawn, suspended, or revoked.

c. The compromise or suspected compromise of a container or its combination, or discovery of a container left unlocked and unattended.

d. At other times when considered necessary by the FSO or CSA.

5-307. Repair of Approved Containers. Repairs, maintenance, or other actions that affect the physical integrity of a security container approved for storage of classified information shall be accomplished only by appropriately cleared or continuously escorted personnel specifically trained in approved methods of maintenance and repair of containers.

5-308. Automated Access Control System. The Automated Access Control System used at the 821 Grier Drive Facility is an approved MDI card access system and approved MDI alarm system.

Section 4. Transmissions

5-400. General. Classified material is transmitted outside the facility in a manner that prevents loss or unauthorized access.

5-401. Preparation and Receipting.

a. Classified information to be transmitted outside of a facility shall be enclosed in opaque inner and outer covers. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification of its contents. A receipt shall be attached to or enclosed in the inner cover. The receipt shall identify the sender, the addressee and the document, but shall contain no classified information. It shall be signed by the recipient, returned to the sender.

b. A suspense copy will be retained in Document Control to track transmitted documents until a signed copy of the receipt is returned. If the receipt is not received within 30 days a tracer copy is sent.

c. When the material is of a size, weight, or nature that precludes the use of envelopes, the materials used for packaging shall be of such strength and durability to ensure the necessary protection while the material is in transit.

5-402. TOP SECRET Transmission Outside the Facility. TOP SECRET material shall be transmitted by the following methods:

a. A designated courier or escort cleared for access to TOP SECRET information.

b. By electrical means over approved secured communications.

5-403. SECRET Transmission Outside the Facility. SECRET material shall be transmitted by one of the following methods.

a. By the methods established for TOP SECRET.

b. U.S. Postal Service Express Mail and U.S. Postal Service Registered Mail.

c. Other methods as directed, in writing, by the GCA.

5-404. CONFIDENTIAL Transmission Outside the Facility. CONFIDENTIAL material shall be transmitted by the methods established for SECRET material or by U.S. Postal Service Certified Mail.

5-405. Addressing Classified Material.

a. The inner container will be addressed, return addressed, carefully sealed, and plainly marked with the classification of the contents. Warning notices will be used where required.

b. The outer container will be addressed, return addressed, and carefully sealed. Markings or notations that would indicate the contents are classified will not be used. Should any markings on the inner container be visible, additional wrapping of the outer container is required to conceal the markings.

5-406. Use of Couriers. Employees who are designated couriers, handcarriers and escorts shall be:

a. Briefed on their responsibility to safeguard classified information.

b. Possess an identification card, which contains our Company Name and the name and a photograph of the employee.

c. Briefed on retaining the classified material in his or her personal possession at all times. Arrangements shall be made in advance if overnight storage is required.

c. If the classified material is being handcarried to a classified meeting, a Receipt for Material will accompany the package to and meeting and returning to the facility.

e. Courier will be provided an authorization letter provided by the Security Department.

5-407. Use of Commercial Passenger Aircraft for Transmitting Classified Material. Classified material may be handcarried aboard commercial passenger aircraft by cleared employees with the approval of the FSO. The employee will be provided with written authorization. The written authorization shall:

a. The full name, SSN, and courier card #.

b. Describe the material being handcarried and request that it be exempt from opening.

c. Identify the points of departure, destination and known transfer points.

d. Include the name, telephone number and signature of the FSO.

e. The Courier Card will provide the full name, date of birth, height, weight, and signature of the courier.

5-408. U.S. Postal Mailing. A U.S. Postal mailing channel, approved by the PSO has been established.

a. U.S. Postal Service certified mail may be used for CONFIDENTIAL/SAR. "FOR OFFICIAL USE ONLY" and unclassified HVASACO material may go by First Class mail. P.O. Boxes should be used only with prior approval of the PSO.

b. Except for TS, USPS Express mail can be used for overnight transmission.

c. These means of transmitting selected special access materials is in addition to, not a replacement for, other transmission means previously approved for such material. Secure facsimile remains the preferred method of transmission.

d. Any problem, misdelivery, loss, or other security incident shall be reported immediately to the CPSO.

e. Use overnight delivery only when:

1. Approved by the PSO.

2. It is necessary to meet program requirements.

3. It is essential to mission accomplishment.

4. Time is of the essence, negating other approved methods of transmission.

5. Government program management considers this method to be cost-effective.

f. Packages must meet the carrier's size and weight limitations or other similar restrictions.

g. Wrapping, addressing, and receipting procedures previously described IN 5-401.a. will be used. The commercial express carrier envelope is not considered the second envelope for double-wrapping; the carrier envelope becomes the third wrap.

h. The Waiver of Signature and Indemnity on the U.S.P.S. label will not be executed to ensure direct delivery to the recipient.

i. The release portion on commercial carrier forms will not be executed.

j. Ensure an appropriate recipient is designated and available to receive material.

k. Do not disclose to the express service carrier that the package contains classified material.

l. When using an U.S. Government approved contract carrier, packages will only be sent on Monday through Thursday to ensure that the carrier does not retain a classified package over a weekend.

5-409. TOP SECRET Transmission. TOP SECRET(TS) SAP will be transmitted via secure data transmission or via Defense Courier Service unless other means have been authorized by the PSO.

5-410. Secure Facsimile and /or Electronic Transmission. Secure facsimile and/or electronic transmission encrypted communications equipment may be used for the transmission of Program classified information with approval in writing from the PSO or other Government cognizant security reviewing activity.

a. Transmissions of classified Program material by this means may be receipted for by an automated system generated message that transmission and receipt have been accomplished.

b. For TOP SECRET documents a receipt on the secure facsimile may be required by the PSO.

c. Facsimile terminals equipped with an automatic polling function will not be used.

d. Voice contact with the recipient will be established before sending Top Secret messages via secure fax. The STU II must indicate Top Secret and a receipt will be received at the time of transmission. Included in the receipt will be the date, copy number, subject, and signature of the recipient.

Section 5. Disclosure

5-500. General. Classified information is disclosed only to authorized persons. Public release of SAP information is not authorized without written authority from the Government as provided for in U.S. Code, Titles 10 and 42. Any questions concerning disclosure of classified information should be directed to the Security Department. Any attempt by unauthorized personnel to obtain Program information and sensitive data will be reported immediately to the Government Program Manager (GPM) through the PSO using approved secure communications channels.

a. Do not release information concerning programs or technology to any non-program-accessed individual, firm , agency or Government activity without the Security Manager's or PSO's approval. Do not include information concerning SAPs in general or unclassified publications, technical review documents, or marketing literature. Submit all material proposed for release to the GPM or PSO 60 days before the proposed release date. After an approval is received for public release, additional case-by-case requests to release identical data are not required.

b. NOTE: Public release of information includes any form of, or anything related to, program information,items, or technology-classified or unclassified.

c. Submit any program information intended for discussion at symposia, seminars, conferences, or other form of non-program meeting to the GPM or PSO for review and approval 60 days before intended attendance and release.

d. Program history, system technological advances, operational concepts, special management functions and techniques, and relationships with non-DoD activities remain classified, requiring special access authorization. The PSO controls disposition and access to historical material.

5-501. Disclosure to Employees. Classified information is disclosed to cleared employees as necessary for the performance of tasks or services essential to the fulfillment of a classified contract or subcontract.

5-502. Disclosure to Subcontractors. Classified information is disclosed to a cleared subcontractor when access is necessary for the performance of tasks or services essential to the fulfillment of a prime contract or a subcontract.

Section 6. Reproduction

5-600. General. Reproduction of classified material will be done on a designated reproduction machine by cleared employees.

5-601. Reproduction Procedures.

a. The Minolta EP 8603 is the designated reproduction machine for classified material. This machine is located in Room 207 at the 821 Grier Drive facility. A notice is posted indicating that this machine is the only machine authorized for classified reproduction.

b. The copier, on the second floor, is the only copier cleared for classified copying. It is locked on the weekends. Arrangements can be made, by contacting the DCC, to use the copier after hours.

c. EG&G personnel have been assigned a security code, by the DCC, that enables the copier. Contact the DCC to obtain the code.

d. Rules for using the designated copier will be conspicuously posted near the machine.

e. Reproduction of classified will be coordinated with the Document Control Coordinator or the FSO.

f. Copies will be entered into the Reproduction Log to reflect date made, unclassified description, original log number, and number of copies made.

g. Three blank copies will be run after completion of classified reproduction to ensure no originals or copies remain in the machine and no residual image is left on the machine.

5-602. Limitations.

a. TOP SECRET documents shall be reproduced only as necessary in the preparation and delivery of a contract deliverable.

b. TS material will be reproduced upon approval of the PSO.

5-603. Marking Reproductions. All reproductions of classified material shall be conspicuously marked with the same classification markings as the material being reproduced. Copies of classified material shall be reviewed after the reproduction process to ensure that these markings are visible.

Section 7. Disposition and Retention

5-700. General. Classified material shall be reviewed on a continuing basis to determine the absolute minimum quantity necessary to accomplish the mission. CPSOs may be required to inventory, dispose of, request retention, or return for disposition all classified SAP-related material (including AIS media) at contract completion and/or close-out.

a. Request for proposal (RFP), solicitation, or bid and proposal collateral classified and unclassified material contained in program files will be reviewed and screened to determine appropriate disposition. Disposition recommendations by categories of information or by document control number, when required, will be submitted to the PSO for concurrence. Requests for retention of classified information (SAP and non-SAP) will be submitted to the Contracting Officer, through the PSO for review and approval. Requirements for storage and control of materials approved will be approved by the PSO.

5-701. Retention of SAP Material. EG&G will submit a request to the Contracting Officer (CO), via the PSO, for authority to retain classified material beyond the end of the contract performance period when required.

5-702. Destruction. Appropriately indoctrinated personnel shall ensure the destruction of classified SAP data. Nonaccountable waste and unclassified SAP material may be destroyed by a single Program-briefed employee. The destruction of accountable classified material must be conducted by at least two program accessed individuals. Material shall be destroyed as soon as practical after it has served the purpose for which it was:

a. Released by the Government.

b. Developed or prepared by EG&G Technical Services.

c. Retained after completion or termination of the contract.

5-702. Methods of Destruction. Classified material will be destroyed beyond recognition so as to preclude reconstruction of the information in whole or in part. Material removed from the facility for destruction must be destroyed the same day. Methods used may be.

a. Burning

b. Melting

c. Mutilation

d. Chemical decomposition

e. Pulping

f. Disintegration

g. Pulverizing

h. Shredding (approved Intimus 007 Shredder located in Room 208 at Grier Drive facility)

Classified materials, manufacturing waste and by products will be destroyed by procedures coordinated with the PSO.

5-703. If materials are removed from a SAPF for destruction at a central activity, ensure that materials are destroyed the same day they are removed.

5-704. Destruction Records. Destruction certificates will be prepared for all classified material, regardless of classification when destroyed. Destruction certificates will contain:

a. Date of destruction.

b. Unclassified identification

c. Signatures of the employee and witness, signed at the time of destruction.

d. Both individuals are required to know, through their personal knowledge, that the material was destroyed.

5.705. Classified Waste. Classified waste shall be destroyed as soon as practical. This applies to all waste material containing classified information. Pending destruction, classified waste shall be safeguarded as required for the level of classified material involved. Receptacles utilized to accumulate classified waste shall be clearly identified as containing classified material. This concept shall be applied to preliminary drafts, carbon sheets, carbon ribbons,

plates, stencils and masters. Safeguard typewriter and computer equipment ribbons used in transcribing classified material in the manner appropriate for the classification category involved. This material shall be marked as PROTECT AS (enter appropriate classification).

a. All material, including unclassified, generated in program areas is considered as classified waste and destroyed accordingly.

b. The PSO shall direct the destruction of waste products generated by laser and color output devices.

Section 8. Construction Requirements.

5-800. General. All SAPF construction and modifications must be approved by the PSO. Construction requirements and modifications will be in accordance with DCID 1/21.

a. Guard response to alarms will be in accordance with DCID 1/21.

b. Response personnel will remain at the scene until released by the CPSO or designated representative.

c. NOTE: The CPSO will immediately provide notification to the PSO if there is evidence of forced entry, with a written report to follow within 72 hours.

5-801. Prohibited Items. Items that constitute a threat to the security integrity of the EG&G facility (e.g., cameras or recording devices) are prohibited unless authorized by the CPSO.

a. The following items do not pose a threat to the EG&G facility and can be taken into and out of the facility without approval:

1. Hearing aids, heart pacemakers, and motorized wheelchairs.
2. Amplified telephone handset and teletypewriters (when used by the hearing impaired).
3. Audio and video equipment with no record capability.
4. Compact disk players.
5. Televisions and AM/FM radios.
6. Receive-only beepers.
7. Receive-only pagers.

b. The following items may not be introduced into the EG&G facility:

1. Personally-owned computers and associated media.
2. Personally-owned photographic, video and audio recording equipment.
3. Two-way audio RF (e.g. two-way radios and cellular phones) transmitting devices that are government or company owned for program use can be

authorized by the CPSO. NOTE: Two-way audio RF transmitting devices can be authorized by the PSO when required for operational necessity.

4. Cameras and film, unless specifically approved by the CPSO for a program mission requirement, (e.g., badge issuance or documenting test results).
5. Other emanating and reproducing devices identified by the CPSO.

c. Personally-owned equipment brought into EG&G facilities is subject to inspection at any time. Any device removed from the EG&G facility also may be subjected to an inspection.

Section 9. Intrusion Detection Systems.

5-900. General. This section applies to all the IDS at EG&G downtown facilities to include 821 Grier Drive; 900 Grier Drive Suite A; and 2920 N. Green Valley Parkway Suite 412. All alarm systems installations conform to the standards set forth in DCIC 1/21.

5-901. CSA Approval. As of this writing both 821 and 900 Grier Drive have been approved by the PSO based on the criteria in DCID 1/21. 2920 N. Green Valley Parkway Suite 412 is in the process of installing the IDS in accordance with DCID 1/21 standards.

5-902. Central Monitoring Station.

a. The IDS at 821 Grier Drive is connected to the central monitoring station at the McCarran Airlift facilities at 5400 S. Haven Drive. This facility has been approved by the PSO as a Government Contractor Monitoring Station. The central monitoring station for the 900 Grier Drive and 2920 N. Green Valley Parkway facilities is a UL approved cleared commercial central station operated by ALARMCO.

b. All monitors at the central stations are trained and cleared to at least the SECRET level and are on duty when the IDS is in operation.

c. Whenever the central monitoring station detects a malfunction or tampering with the IDS a cleared company employee will be assigned to the alarmed facilities until the repairs are complete.

d. When an IDS is used, it will be activated immediately at the close of business at the alarmed area or container. A record will be maintained at all three facilities identifying the person responsible for setting and deactivation the IDS. Each failure to activate or deactivate shall be reported to the FSO. Records will be maintained for 30 days.

e. Records shall be maintained for 90 days indicating time of receipt of alarm; name of security force personnel responding; time of dispatch to facility; time security

force personnel arrived; nature of alarm; and what follow-up actions were accomplished.

5-903. Investigative Response to Alarms.

a. Type of Response Force.

1. For 821 Grier Drive the response force will be trained proprietary security force personnel, cleared to the SECRET level. This force will be available at all times when the IDS is operational.

2. For 900 Grier Drive and 2920 N. Green Valley Parkway both Alarmco uncleared guards and company proprietary cleared guards will be dispatched to the facilities.

3. Uncleared guards dispatched by Alarmco shall remain on the premises until a designated, cleared representative of the facility arrives, or for a period of not less than 1 hour, whichever comes first. A complete report must be provided by the central monitoring station in accordance with Chapter 5, Section 9, paragraph 5-903 of the NISPOM to the CSA.

4. Subcontracted guards must be under contract with either the installing alarm company or the cleared facility.

b. Response Time: The response time for all three facilities will be 15 minutes for EG&G response personnel. NO EXCEPTIONS.

5-904. Installation. The IDS systems at all three company facilities have been installed by Alarmco, a UL listed alarm company, approved by the CSA. The DCMS and Alarmco both provide protective signaling security lines.

5-905. Certification of Compliance. Alarmco has issued both 900 Grier Drive and 2920 N. Green Valley Parkway a current UL Certificate for the appropriate category of service. These certificates are on file in the Security Office at Grier Drive. The CSA and the PSO have approved the IDS at 821 Grier Drive.

CHAPTER 6. VISITS AND MEETINGS

Section 1. Visits

6.100. General. A Classified Visit Request for all program visits will be made prior to a visit to a Program facility. When telephone requests are made, a secure telephone will be used whenever possible

a. Uncleared visitors are issued a Visitor badge and continuously escorted in all cleared areas of the facility.

b. Program personnel are notified when an uncleared person is entering the area.

6.101. Visit Request Procedures. All visit requests are sent only via approved channels. In addition to the NISPOM, the following additional information for visits to a SAPF will include:

a. Name and telephone number of individual to be visited.

b. Designation of person as a Program courier when applicable.

c. Verification signature of FSO or designated representative that the visit request information is correct.

6.102. Termination and/or Cancellation of a Visit Request. If a person is debriefed from the Program prior to expiration of a visit certification, or if cancellation of a current visit certification is otherwise appropriate, the FSO or his/her designated representative will immediately notify all recipients of the cancellation or termination of the visit request.

6.103. Visit Procedures.

a. An official photograph of identification such as a valid driver's license is required.

b. When a visit extends past the date on the visit request, a new visit request is not required if the purpose remains the same as that stated on the current visit request to a specific SAPF.

c. When a rescheduled visit occurs after a visit request has been received, the visit request will automatically apply if the visit is rescheduled within thirty days and the purpose remains the same.

d. It is the responsibility of the host FSO to contact the visitor's FSO should the visitor plan to hand-carry classified material. FSOs will use secure means for notification. When persons return to their facility with SAP material, they will relinquish custody of the material to Document Control. Arrangement will be made to ensure appropriate overnight storage and protection for material returned after close of business.

e. Instances where entry to a SAPF by non-Program-briefed personnel is required, they will complete and sign a visitor's record and will be escorted by a Program-briefed person at all times. Sanitization procedures will be implemented in advance to ensure that personnel terminate classified discussions and other actions and protect SAP information whenever a non-briefed visitor is in the area.

6-104. Visitor Record. A visitor sign-in and sign out record for all accessed program visitors. This record shows the visitor's name, SSN, organization or firm, date, time in and out, and sponsor on the log.

Section 2. Meetings

6.200. General. This Section applies to a conference, seminar, training or other such gathering during which classified information is disclosed.

6.201. Location of Meetings. Classified meetings will only be held in classified conference rooms approved for classified discussions by the CSA and SAP conference rooms approved for SAP discussions approved by the PSO at all three company facilities.

a. All persons in attendance at classified sessions shall possess the required clearance and need-to-know for the information to be disclosed. This information can be submitted on the Visit Requests when required.

b. The names of all authorized attendees or participants must be submitted to the ACO prior to the meeting. The ACO will verify the attendee's identity and clearance information before admitting to the Conference room.

c. Individuals making presentations at meetings shall provide sufficient classification guidance to enable attendees to identify what information is classified and the level of classification. Classified information must be authorized for disclosure in advance by the Government Agency having jurisdiction over the information to be presented. Classified presentations shall be delivered orally and/or visually. Copies of classified presentations or slides, etc. shall not be distributed at the classified meeting, and any classified notes or electronic recordings of classified presentation shall be classified, safeguarded, and transmitted as required by the NISPOM.

d. All attendees will be required to sign the sign-in log in the classified conference room. Physical security measures also shall provide for control of, access to, and dissemination of, the classified information to be presented and shall provide for secure storage capability, if required. Also when authorized, the FSO may request a Technical Surveillance Countermeasures (TSCM) survey when SAP information is to be discussed.

6-202. Disclosure Authority at Meetings. A contractor desiring to disclose classified information at a meeting shall furnish a copy of the disclosure authorization to the Government Agency sponsoring the meeting. Each contractor that desires to disclose classified information at a meeting is responsible for requesting and obtaining disclosure approvals.

6-203. Requests to attend Classified Meetings. Before a company employee can attend a classified meeting, the FSO shall certify the PCL of the employee and provide justification why the employee requires access to the classified information. This information can be provided on the Visit Request.

CHAPTER 7. SUBCONTRACTING

Section 1. Prime Contractor Responsibilities. Sub-Contractors will be issued a form DD254 stipulating the mandatory security regulations for the applicable contracts.

a. All prospective subcontractor personnel will have the appropriate security clearance and meet the investigative criteria as specified in this Supplement prior to being briefed into a SAP.

b. Prior to initiating contact with a prospective vendor or subcontractor, the FSO will complete a SAP Format 13, Subcontractor/Supplier Data Sheet, for submission to the PSO. The FSO will include the reason for considering a vendor and attach a proposed DD Form 254 to the SAP Format 13. The DD Form 254 shall be tailored to be consistent with the proposed support being sought. The DD Form 254 may be classified based on the information contained therein.

c. Contract Security Classifications Specifications (DD254) prepared by EG&G will coordinate with the GPM/PSO and contracting officer prior to transmitting to the subcontractor. The DD254 prepared by EG&G will be forwarded to the GPM/PSO and contracting officer for coordination and signature.

AUTOMATED INFORMATION SYSTEM STANDARD PROCEDURES

CHAPTER 8. AUTOMATED INFORMATION SYSTEM SECURITY

INTRODUCTION: This AISSP covers TOP SECRET/SAR, SECRET/SAR and collateral SECRET AIS.

Section 1. Responsibilities

8-100. Administration. The Customer is the Cognizant Security Agency (CSA) responsible for the accreditation of the AIS.

a. This is the AISSP dated 15 February 2000 for
EG&G Technical Services
821 Grier Dr.
Las Vegas, NV 89119

AIS equipment is located in Rooms 104, 105, 110, 213, 214, 215, 218,

b. The Facility Security Officer (FSO), Greg Rentchler, (702) 361-1660 X1044, secure (702) 361-1642 X has overall responsibility for the administration of the security program for the facility and appointment of an Information System Security Representative (ISSR).

c. Charlotte Smith, (702) 361-1660 X1045, secure (702) 361-1642 X1202 acting as the ISSR, is the primary point of contact for all matters relating to AIS Security.

8-102. Purpose. This document, which supplements EG&G Technical Services Facility Security Manual, provides instructions for the safeguarding of classified information while resident within or being processed by an Automated Information System (AIS). This AIS Security Plan (AISSP) has been written in accordance with DOD 5220.22-M, "National Industrial Security Program Operating Manual, (NISPOM)" dated January 1995.

a. Scope. This document is applicable to those systems approved for processing in the dedicated mode of operation. It requires that all users of the system have a Personnel Security Clearance, special briefings, and need-to-know for all information stored or processed by the AIS at the time of their access.

Section 2. SAPF DESCRIPTION.

8.200. Physical Environment. EG&G Technical Services 821 Grier Drive Facility is accredited and approved to process and store classified information. The Facility is cleared to the Top Secret level. Facility Cage Code 3H110. The facility is approved for storage of hard

disk drives, diskettes, tapes, printouts, and other material. The following are the only areas approved for open storage:

a. Room 104
b. Room 106 (SCIF)

The only unattended processing approved is in Room 104.

8-201. Floor Layout. See attachments A, B, C floor plan.

8-202. SAPF Access. There is an Access Control Officer on duty at the front entrance of the facility from 6 am until 6 pm. Each Closed area is equipped with an MDI alarm system and card access reader. After duty hours the entire facility is alarmed with MDI and card access only.

a. During normal working hours visitors are badged and signed into the facility and escorted into cleared areas (see 1-203 Badging).

Section 3. AIS DESCRIPTION.

8-300. See Attachments A, B, C for description.

8-301. Configuration and Connectivity. See Attachments A, B, and C # 6 network and attached diagram.

8-301. User Access and Operation.

a. Start-up procedures.

1. Remove unauthorized personnel from the AIS area or preclude access to the AIS.
2. Ensure the physical integrity of the area has been verified and any required modifications/controls have been imposed.
3. Obtain from approved storage all classified/protected media and material needed.
4. If applicable, inspect AIS security seals.
5. Install required classified/protected media/material on the AIS as appropriate.
6. Ensure servers are up and network connection is enabled in room 104.
7. Power on and boot the system, verifying no errors.
8. Return to an approved container, all protected/classified material not needed for classified processing.

b. Shutdown Procedures.

1. Ensure all previous processing on the AIS has ceased.
2. Ensure all classified media/material that was created or utilized during the classified processing session is removed from the AIS.
3. Perform an orderly system shutdown.
4. Remove and store in an approved container all classified/protected media/material.
5. Disable the network connection to the servers in room 104.

c. AIS access control.

1. Prior to granting access to an accredited system, the AIS Access Authorization and Briefing Form will be completed and the information verified. This form will serve to certify the user's AIS briefing, clearance level, need-to-know, and required level of AIS accesses and privileges. Following completion of the form, the system administrator or AIS Custodian will establish (if applicable), the user's account in accordance with the specifications of the form.

2. User accounts will be terminated in a timely manner whenever a user is no longer employed, has a reduction in level of clearance, or no longer possesses the appropriate need-to-know. The user or his supervisor will be responsible for notifying the ISSR when there is a change in need-to-know. If applicable, the system administrator or AIS Custodian will disable the account and record the date of access termination in the AIS Authorized Users Log.

d. Procedures for the assignment and distribution of passwords. AISs that do not use automated access controls will maintain a hard copy list of authorized users. Systems that utilize passwords for access controls must comply with the following requisites:

1. Passwords will be at least eight characters in length.
2. Passwords must be changed at least every 90 days or upon known or suspected compromise.
3. Passwords will be classified and controlled at the same level of the highest level processed.

e. All security incidents will be immediately reported to ISSR/FSO.

8-302. Audit Trails. A review of audit trails will be done weekly on the following:

a. Log-in and Log off and failed Log-in entries.

b. Large upload and download entries.

c. Any anomolies noted.

d. Audit trails may be generated and maintained in either hard copy or magnetic media form. If maintained off-line on magnetic media the data must be retrievable upon CSA request. Audit trail records shall be retained until reviewed by the CSA or for 12 months.

e. These audits will be recorded on the AIS AUDIT REVIEW LOG.

Section 4. HARDWARE.

8.400. AIS Hardware. See attachments A,B,C form SPF16 for hardware listing.

8-401. Labeling Hardware. All labels will show classification, special access required, classified by line and document control number.

8-402. Maintenance Procedures. If at all possible, maintenance should be performed by cleared personnel with the appropriate need-to-know. Some hardware changes resulting from maintenance may involve reaccredidation, and therefore, require prior notification of the CSA. The following are general procedures to be followed for performing system repairs and/or preventive maintenance.

a. Diagnostic routines will be obtained from the appropriate vendor and protected and controlled to the highest level of processing. Diagnostics shall be utilized by cleared authorized personnel only.
b. When scheduling an outside repair person for maintenance, question them as to the type of equipment/materials they will need for evaluation of the problem. ISSR or AIS Custodian approval must be obtained to bring in maintenance tool, diagnostic equipment, or any other device to be used to service an accredited AIS. Special attention should be given to portable units that contain memory and/or have retention capabilities. These devices may require accreditation by the CSA.
c. All maintenance to the approved AIS equipment must be monitored by authorized personnel and documented in the AIS Change and Significant Action Log. This is regardless of whether the AIS is currently in classified or unclassified mode.
d. All repaired or replacement parts and equipment shall be inspected for foreign devices and tampering.
e. All AIS security functions will be checked following maintenance actions to ensure they are all still enabled and operating properly. This includes such functions as unsuccessful log on attempts, auditing, classified labels, etc.

8-403. Clearance, Sanitization, Declassification, and Destruction Procedures. The sanitization, declassification, and release of media used to process program information

may only be authorized on a case-by-case basis by the PSO and GPM. Only customer-approved equipment and software may be used to overwrite and degauss magnetic media. These products will be tested to assure correct operation before each use, either by inspection or by built-in test devices.

Table 1
Clearing and Sanitization Data Storage

Type Media	Clear	Sanitize
(a) Magnetic Tape		
Type I (coercivity is no greater than 350 Oersteds)	a or b	a, b, or destroy
Type II (coervicity is no greater than 750 OE)	a or b	b or destroy
Type III (coercivity over 750 Oe)	a or b	Destroy
(b) Magnetic Disk Packs		
Type I		a, b, or c
Type II		b or c
Type III		Destroy
(c) Magnetic Disk Packs		
Floppies	a, b, or c	Destroy
Bernoulli's	a, b, or c	Destroy
Removable hard Disks	a, b, or c	a, b, c, or destroy
Non-Removable Hard Disks	c	a, b, c, or destroy
(d) Optical Disk		
Read Only		Destroy
Write Once, Read Many (Worm)		Destroy
Read Many, Write Many	c	Destroy

These procedures will be performed by or as directed by the ISSR.

a. Degauss with a Type I degausser.
b. Deguass with a Type II degausser.
c. Overwrite all locations with a character, its complement, then with a random character. Verify that all sectors have been overwritten and that no new bad sectors have occurred. If new bad sectors have occurred during classified processing, this disk must be sanitized by method a or b described above. Use of the overwrite for sanitization must be approved by the Customer.

Table 2
Sanitizing AIS Components

TYPE	PROCEDURE
Magnetic Bubble Memory	a, b, or c
Magnetic Core Memory	a, b, or d
Magnetic Plated Wire	d or e
Magnetic-Resistive Memory	Destroy
Solid State Memory Components	
Random Access Memory (RAM) (Volatile)	f, then j
Nonvolatile RAM (NOVRAM)	l
Read Only Memory (ROM)	Destroy (see k)
Programmable ROM (PROM)	Destroy (see k)
Erasable Programmable ROM (EPROM)	g, then d and j
Electronically Alterable PROM (EAPROM)	h, then d and j
Electronically Erasable PROM (EEPROM)	i, then d and j
Flash EPROM (FEPROM)	I, then d and j

These procedures will be performed by or as directed by the ISSR.

a. Degauss with a Type I degausser.
b. Degauss with a Type II degausser.
c. Overwrite all locations with any character.
d. Overwrite all locations with a character, its complement, then with a random character.
e. Each overwrite will reside in memory for a period longer than the classified data resided.
f. Remove all power, including batteries and capacitor power supplies, from RAM circuit board.
g. Perform an ultraviolet erase according to manufacturer's recommendation, but increase time requirements by a factor of 3.
h. Pulse all gates.
i. Perform a full chip erase. (See Manufacturer's data sheet.)
j. Check with Customer to see if additional procedures are required.
k. Destruction required only if ROM contained a classified algorithm or classified data.
l. Some NOVRAM are backed up by a battery or capacitor power source; removal of this source is sufficient for release following item f procedures. Other NOVRAM are backed up by EEORIN which requires application of the procedures for EEPROM (i.e., I, then d and j).

8-404. Transferring Data to/from a Classified Computer to Less-Classified or Unclassified Media.

I. An individual authorized by the ISSR must perform or oversee the process. This authorization must be in writing, and kept on file by the ISSR. ISSSR's will issue this authorization after users have demonstrated that they understand this transfer procedure.

II. The unclassified data will be written to factory fresh or verified unclassified media.

III. Review the data using its parent application. For example, review a word processor document using a word processor, a spreadsheet document using a spreadsheet program, etc.

A. Review the entire document, not just "random samples".

B. For word processing documents, take care to also review headers and footers, which may contain classification markings.

C. The objective of this step is to review the data which is visible from within the application. Step 5 will review the data which is not visible from within the application.

IV. If the document is not a text or graphic file, convert it to a text or graphic file.

A. This step is required because many proprietary document formats hide unintended information, to include contents of previous revisions, other unrelated files, and arbitrary contents of memory. This information may not be visible from within the application. Furthermore, this data may not be in text form, so that it cannot be easily reviewed and determined to be at the intended classification level.

B. Guidance for specific document types:

1. Microsoft Word documents:

a. If transferring a Microsoft Word document, save it in Rich Text Format or in Text format.

WARNING: the native Microsoft Word .DOC file format has multiple security holes which allow the inadvertent inclusion of data from previous revisions, from other

unrelated files, and from other data in your computer's memory. Avoid transferring .DOC files from a classified computer.

2. Spreadsheets and databases:

   a. Spreadsheet and database files cannot be transferred as-is. Export these documents as text, then transfer the text files only.

3. Microsoft Powerpoint documents:

   a. Microsoft Powerpoint documents consist mainly of data which cannot be interpreted by human reviewer. There is also a bug in some versions of Microsoft Powerpoint which writes arbitrary pieces of memory into a Powerpoint document. To avoid these risks, save the Powerpoint document outline as text, then transfer the text outline only. Reconstruct the Powerpoint briefing on the less-classified system.

4. Graphics files:

   a. Graphic files in the JPEG and GIF format can be reviewed using standard image viewers and safely transferred.

5. Executable files:

   a. Executable program files are typically very long and almost entirely unintelligible. They should not be routinely transferred. Obtain the program from unclassified sources instead.

   b. Programmers: Instead of transferring executables, transfer the text source code from the classified system and recompile it on the less-classified system.

6. Other files types: Other file types may be transferred if the entire contents of the file can be reviewed and understood. If a file contains unintelligible data, it should be assumed to be classified system-high.

a. However, a file may be transferred without review if the file was imported from a less-classified system and is verifiably unchanged.

b. On a case-by-case basis, ISSR's may authorize the transfer of files containing unintelligible data, when the ISSR assesses that there is a negligible risk that the unintelligible data is classified.

V. Completely review the entire file using a low-level viewer:

A. Graphics files may be reviewed with a graphics file viewer.

1. Warning: Some graphics file format contain imbedded text comment fields which may not be displayed by most graphics file viewers. This is true of GIF and TIFF files. These files should also be reviewed using a text file viewer.

B. For all other files, use a text file viewer. Use Microsoft "Write" or any other program which displays the entire raw contents of the file.

1. To use Microsoft Write to review the file, follow these steps:

a. From Program Manager, double-click on the "Write" icon (usually found in the "Accessories" program group).

b. From the "Write" File menu, choose "Open", then select the file you wish to review.

c. When prompted for "Conversion" or "No Conversion", choose "No Conversion".

d. The file will then be displayed. Scroll through the entire file, looking for classified information.

e. Note that some displayed lines will be longer than the screen width. Make sure you scroll horizontally to view these long lines in their entirety.

f. After reviewing the entire file, "Quit" without saving.

VI. Use the Secure Copy utility from the AIA COMPUSEC Toolbox to copy the reviewed file onto the Unclassified diskette disk. (If you do not have the AIA

COMPUSEC Toolbox installed on your machine, see your ISSR for a copy, or download from our home page http://www.aia.ic.gov/infoprotect.

A. Using the Secure Copy program, select the files that you wish to copy to the floppy. (On-line help for Secure Copy is available by pressing F1).

B. Immediately before the copy operation (i.e. after the files have been selected, but before pressing "F10" of the DOS version, or clicking on copy button of the NT version to execute the copy command), eject the blank, Unclassified diskette, write-enable it, then re-insert it.

VII. Use the FLUSH program from AIA COMPUSEC Toolbox to overwrite all unused space on the floppy.

A. As soon as the flush operation is complete, eject the floppy disk, write-protect it, then re-insert it.

VIII. Use the BUSTER program from the AIA COMPUSEC Toolbox to scan the diskette for any classification markings.

A. WARNING: BUSTER is nothing more than a text keyword search – it won't detect unlabeled classified information, or classified information in compressed files, or non-text classified information. However, it is a useful "last-ditch" check to guard against mistakes.

IX. If the diskette will be sent to another unit, virus-scan the diskette before sending it.

X. Create an administrative record of the transfer, specifying:

A. Data being released.

B. Personnel involved.

C. Date of release.

8-405. Transferring data from a classified Unix system to a less-classified (or unclassified) tape or floppy:

I. These procedures should be tailored for the local environment. In particular, the Unix commands listed herein are for illustration only and must be modified to account for the Unix version, hardware configuration, and software installation specifics.

II. An individual authorized by the ISSR must perform or oversee the process. This authorization must be in writing, and kept on file by the ISSR. ISSR's will issue this authorization after users have demonstrated that they understand this transfer procedure.

III. The target tape or floppy should be factory fresh.

IV. Create a designated source directory for the transfer, using the Unix "mkdir" command:

```
mkdir source_directory
```

A. Rationale: This will establish a blank directory. The files to be copied to tape/floppy will first be moved here. This two-step process helps ensure that only the intended files are copied.

V. Move all files to be copied to tape into the designated source directory.

VI. View the entire contents of all files in the designated directory, verifying that the entire contents of the files are at the desired security classification. Persons performing the review must be familiar with the classification guidelines pertaining to the subject matter. This review must be administratively documented.

A. For text files: view the file using software which displays the entire contents of the file. Any unintelligible data must be assumed to be classified system-high.

B. For graphics or movie files: review the file using an appropriate graphics file viewer. Ensure that the file format does not include internal annotations or other additional data (if present, this information can only be viewed with a specialized viewer, and poses a significant threat of inadvertent disclosure). If unfamiliar with the internal structure of the graphics file, do not assume it contains no hidden data – obtain competent technical advice before proceeding.

C. Other non-text files: the classification of non-text, non-graphics files cannot generally be determined without intensive technical analysis. Such files must be assumed to be classified system-high. Files in this category include binary database files, compressed archives, and executable code.

1. In the case of executable files, recommend reviewing and downgrading the source code, then transferring the source code to a lower-classified machine for re-compilation.

2. In the case of binary database files, recommend exporting the data to ASCII text format, then reviewing and downgrading the text.

3. Compressed archives should be reviewed and transferred uncompressed.

VII. Perform an automated "Dirty Word" scan of the entire contents of the source directory. A perl script is one way to accomplish this scan.

VIII. Load the write-enabled tape or floppy into the drive. Warning: Do not load the write-enabled media until ready to immediately go on to the next step.

A. Rationale: this reduces the possibility of an inadvertent write to the media (e.g. by another user or process, or due to inadvertent/incorrect command).

IX. Use the "Secure/Tar" (S/Tar) utility to create and write an archive of the source directory to the media. The Unix command sequence will be as shown below (the exact command may very depending on the Unix version, machine configuration, media used and where/how S/Tar was intstalled):

mt –f /dev/rst0 rew	Ensure tape is rewound (not required if using floppy)
star cvg /dev/rst0 /source_directory	Create Tar file on tape

A. Note: S/Tar should be used in preference to the Unix "tar" command. Tar pads the end of files with arbitrary data from the system – that padding data may be classified. This problem is particularly acute with files that are less than one block long (files which are more than one block long are usually padded with data from the file itself). S/Tar avoids this problem by padding files with zeros.

X. Immediately after the above operation completes, unload and write-protect the media. Then re-load the write-protected media into the drive.

XI. Verify that the media contains the expected data by printing a directory of the Tar file:

mt –f /dev/rst0 rew	Ensure tape is rewound (not required for floppy)
tar tvf /dev/rst0 | 1pr	Print directory of file (| 1pr may be omitted for on-screen review)

XII. The output of the above command should match the contents of the source directory. To verify that they match, compare the output of the above command with the directory printed by the following command:

ls –alr /source_directory |lpr (| lpr may be omitted for on-screen review)

A. Ensure that the date, time, and size information are as expected. If any unintended data was copied, the target tape should be considered classified system-high.

B. Rationale: the files which were unintentionally copied may be classified.

XIII. Apply the appropriate security classification label to the tape or floppy.

XIV. Create an administrative record of the transfer, specifying:

A. Data being released.

B. Personnel involved.

C. Date of release.

8-406. Transferring data to a classified PC-compatible system from a less-classified (or unclassified) floppy:

I. An individual authorized by the ISSR must perform or oversee the process. This authorization must be in writing, and kept on file by the ISSR. ISSR's will issue this authorization after users have demonstrated that they understand this transfer procedure.

II. On the classified system, verify the proper functioning of the write-protect mechanism by attempting to write to a write-protected scratch diskette. The attempt should fail.

III. Write protect the less-classified (or unclassified) diskette containing the data to be transferred.

A. On 3-1/2" floppy diskettes, the diskette is write-protected when the write-protect tab is OPEN.

B. On 5-1/4" diskettes, the diskette is write-protected when the write-protect tab is COVERED.

IV. Insert the write-protected diskette into the classified system.

V. Virus scan all files on the diskette, using an up-to-date virus scanner.

VI. Copy the data from the less-classified diskette onto the classified system.

VII. Remove the diskette from the system, visually checking that the diskette is write-protected.

VIII. Make an administrative record of the transfer, listing:

A. Date being uploaded.

B. Personnel involved.

C. Date of upload.

8-407. Transferring data to a non-PC-compatible system from less-classified (or unclassified) media:

I. An individual authorized by the ISSR must perform or oversee the process. This authorization must be in writing, and kept on file by the ISSR. ISSR's will issue this authorization after users have demonstrated that they understand this transfer procedure.

II. On the classified system, verify the proper functioning of the write-protect mechanism by attempting to write to write-protected scratch media. The attempt should fail.

III. Virus scan the disk.

IV. Write-protect the less-classified (or unclassified) media containing the data to be transferred.

V. Insert the write-protected media into the classified system.

VI. Copy the data from the less-classified media onto the classified system.

VII. Remove the media from the system, visually checking that the media is write-protected.

A. If the media was not write-protected while in the classified system, the media should be considered classified and marked accordingly.

VIII. Make an administrative record of the transfer, listing:

A. Data being uploaded.

B. Personnel involved.

C. Date of upload.

8-408. Hardware Movement. All classified AIS equipment is brought to Document Control.

a. Equipment is logged out and a Receipt for Material is filled out in duplicate. One is sent with the equipment and one is retained in Document as a suspense copy.

b. Classified equipment is then double wrapped and hand carried by an authorized courier to the destination.

c. SAPF 16 will be updated and transferred with equipment.

Section 5. SOFTWARE.

8-500. Software. The SAPF 16 referencing a master software list will include the name, manufacturer, and version # of all operating system software, application software, and security related software and firmware. Software and firmware developed in support of a contract shall also be listed here, or the contractually imposed software configuration baseline may be referenced. All software, both new and revisions to previously installed software, shall be approved by the reconfiguration in the AIS Change and Significant Action Log and update the AIS Software/Firmware List.

a. **Software Controls.**

1. Contact the ISSR/AIS Custodian for necessary approval prior to loading new software or firmware.

2. Security related software will be validated by the AIS Custodian or designee to confirm that every feature is fully functional before submission for accreditation.

3. From the earliest feasible time, all AIS software will be stored on media that is safeguarded to the highest level of intended processing.

4. All software will be loaded from media which is write-protected when possible.

b. **Software Installation.**

1. Installation and modification of software will be performed by authorized personnel who are knowledgeable of the computer system and the software being installed.

2. Software that is not received directly from the vendor into a protected environment must be virus scanned prior to installation on an accredited system.

3. Installation and testing of operating system and security related software shall be documented in the AIS Change and Significant Action Log. The current software configuration must be reflected in the AIS Software/Firmware List.

c. **Operating Procedures.** Other documents applicable to the operation of the AIS, which include security procedures, shall be reviewed by the ISSR to ensure consistency with this document prior to implementation. When modifications to this document, or other procedures affecting the operation of the AIS are required, the ISSR will be notified. The Security Custodian will make the necessary changes to the applicable list(s) and/or log(s).

Section 6. MEDIA.

8-600. Data Storage Media.

8-601. Labeling and Storing Media. All media is labeled with the classification, special access required, contents of media, classified by line and a document control #. All removable media is stored in GSA approved safes. All non-removable media is stored in approved vaults. All unclassified media is labeled as unclassified.

8-602. Media Movement. Media is brought to Document Control.

a. Media is logged out and a Receipt for Material is filled out in duplicate. One is sent with the equipment and one is retained in Document as a suspense copy.

b. Media is then double wrapped and hand carried by an authorized courier to the destination.

8-603. Media Control. All media is issued a Document Control number from the appropriate Document Control Log; labeled with appropriate classification labels and stored in GSA approved containers.

8-700. AIS Security Awareness Program.

a. **Initial Training Requirements.** Initial security awareness training shall encompass all AIS security requirements for which an individual will be responsible. Depending on job function, responsibilities will vary. Anyone who is designated by the ISSR as an AIS Security Custodian or alternate shall receive briefing as to the custodian responsibilities. AIS users may be briefed by the ISSR or the AIS Custodian. At minimum, authorized AIS users shall be aware of the following items:

1. Company's AIS security policy.
2. Methods for controlling access to the area and the AIS.
3. Limitations on removing AIS hardware and software from the controlled area.
4. Requirements for review of output from the AIS.
5. Procedures for reporting security related incidents.

The user will complete the SAPF 21. The employee responsible for maintaining hardware or software on the AIS must additionally be briefed on hardware and software configuration control and maintenance procedures.

b. **Re-Briefing Requirements**. The ISSR or custodian designee is responsible for giving initial and recurring AIS security briefings. At minimum, re-briefing shall take place when one of the following occurs:

1. An AIS user is directly involved in or responsible for the breech of any AIS security policy.
2. There is a change to the security procedures for which an AIS user is responsible.
3. Annually.

APPENDIX A
RDID

1. INTRODUCTION

This document outlines the security procedures that are to be followed by all RDID personnel utilizing the EG&G facility at 821 Grier Drive and is supplementary to the EG&G Security Standard Operating Procedures (SSOP).

It in no way limits the responsibility of all personnel to properly handle, store, and protect classified material.

2. PERSONNEL

Prior to the removal of any classified material, from storage containers, there must be a minimum of two RDID personnel, who are cleared to the highest classification of the data, present in the facility.

3. INVENTORY

An inventory of all classified material, created by the Document Control Coordinator (DCC), shall be maintained in each safe, kept up to date, and checked weekly.

See attached for a list of responsible individuals.

3.1. *DOCUMENT CONTROL*

All classified material must be checked in through the DCC.

All classified material must have a document control number, assigned by DCC, and then in turn be signed out to the person who will be maintaining the material.

If classified materials are brought into the building during non-duty hours, the materials must be secured and brought into accountability at the earliest possible time prior to use.

3.2 *TEMPORARY REMOVAL*

Classified material leaving the building must have two Receipt For Material forms filled out and one of them signed. The signed copy shall be given to DCC and the other shall accompany the material. If the DCC is not available, leave the signed copy with the ACO or at the ACO desk. An "OUT" card shall be left in place of the material. Blank forms and examples are located in the Document Control Folder of each safe.

When the material is returned, the unsigned copy of the Receipt For Material, that accompanied the material, shall be turned in to DCC and noted that the material has been returned to its original location.

3.3 *PERMANENT REMOVAL*

Classified material leaving the building must have two Receipt For Material forms filled out and one of them signed. The signed copy shall be given to DCC and the other shall accompany the material. If the DCC is not available, leave the signed copy with the ACO or at the ACO desk. A note shall be made on the inventory stating that the material was permanently removed along with the RFM# of the Receipt For Material.

When the material arrives at the destination, sign and return the Receipt For Material and send it to the DCC at the address in the FROM: block of the Receipt For Material.

4. STORAGE

All classified material must be properly stored in approved storage container and cannot be left unattended at any time.

Network servers may be left running unattended in room 104 only.

At no time is the safe door of room 104 to be left open while the room is unattended. If the room is attended, then the outer door must be kept closed. At the end of the day, both doors must be closed and verified that they are locked.

5. MARKING

All classified material shall be marked in accordance with CHAPTER 4 of the SSOP.

6. NETWORK

This network is for engineering development and documentation only. The classification of the network is as briefed. Any non-volatile storage media attached to the network via any method is to be classified at the highest level of the network. The only exceptions are pre-formatted, write protected floppy disks that have data copied to them using the procedures outlined in section 9.2 below.

At no time will the network be left active when there are less than two RDID personnel left in the facility, who are cleared to the level of the network. Prior to this condition, the network must be disconnected in the foyer of room 104 by removing power from the Ethernet repeater that feeds the network outside of room 104.

7. AUDITING

Auditing of all functions shall be maintained through the use of the NT Audit facilities and follow the master AISSP for review requirements..

1. All log on and log off operations shall be audited. This means that the servers must be running prior to operating any computers.

2. All operations on classified files shall be audited. Classified files shall be maintained on NTFS partitions only.

3. All print or plot operations involving classified files shall be audited.

4. A weekly review of audit trails shall be conducted and the audit file shall be saved on the server and maintained for a period of 12 months.

8. COMPUTERS

8.1 *System Security Profile*

All computers shall have a SAPF 16 on record.

8.2 *Declassification*

Declassification procedures shall be performed on all computers, as per SSOP paragraph 8.403.

8.3 *Repair*

All computer equipment that has been attached to the network, or used for classified processing, shall be repaired by RDID personnel.

9. STORAGE MEDIA

9.1 *Hard Disk*

All hard disks that have been in computers attached to the RDID network shall be classified and marked at the level of the network.

9.2 *Floppy Disk*

Any floppy disk that is formatted on a classified system assumes the classification of that system.

9.3 *Zip disk*

Due to the lack of a visual write-protect indicator on the zip disk, all zip disk that are used on classified systems shall assume the classification of the system.

9.4 *CDROM*

Any CDROM that is generated using a PC that is classified shall assume the classification of the system, unless verified..

9.5 *Magnetic tape*

All magnetic tape used on classified computers shall assume the classification of the system, unless verified..

9.6 *Other*

No other storage media are authorized for use on the RDID network without specific permission of the RDID network administrator.

10. PRINTERS / PLOTTERS

All printers and plotters shall be checked at the end of each day to verify that all classified documents have been cleared from the machines.

No printers, plotters, or other output devices are to be used on the network if they have ribbons or other media that can maintain an image of classified data.

11. CHECK LIST

At a minimum, the following shall be incorporated into any “end of day” checklist that is used.

Ensure that all classified material is properly stored in the safe.

Ensure that all printers and plotters are clear of classified documents.

Ensure that all storage media has been removed from all computers and is properly stored.

Ensure that all computers, printers, and plotters have been declassified.

Physically disconnect network hub in Room 104.

APPENDIX B
RDF

1. INTRODUCTION

This document outlines the security procedures that are to be followed by all RDF personnel utilizing the EG&G facility at 821 Grier Drive and is supplementary to the EG&G Security Standard Operating Procedures (SSOP).

It in no way limits the responsibility of all personnel to properly handle, store, and protect classified material.

2. PERSONNEL

Prior to the removal of any Top Secret material, from storage containers, there must be a minimum of two RDF personnel, who are cleared to the highest classification of the data, present in the facility.

3. INVENTORY

An inventory of all classified material, created by the Document Control Coordinator (DCC), shall be maintained in each safe, kept up to date, and checked weekly.

See attached for a list of responsible individuals.

3.1. *DOCUMENT CONTROL*

All classified material must be checked in through the DCC.

All classified material must have a document control number, assigned by DCC, and then in turn be signed out to the person who will be maintaining the material.

If classified materials are brought into the building during non-duty hours, the materials must be secured and brought into accountability at the earliest possible time prior to use.

3.2 *TEMPORARY REMOVAL*

Classified material leaving the building must have two Receipt For Material forms filled out and one of them signed. The signed copy shall be given to DCC and the other shall accompany the material. If the DCC is not available, leave the signed copy with the ACO or at the ACO desk. An "OUT" card shall be left in place of the material. Blank forms and examples are located in the Document Control Folder of each safe.

When the material is returned, the unsigned copy of the Receipt For Material, that accompanied the material, shall be turned in to DCC and noted that the material has been returned to its original location.

3.3 *PERMANENT REMOVAL*

Classified material leaving the building must have two Receipt For Material forms filled out and one of them signed. The signed copy shall be given to DCC and the other shall accompany the material. If the DCC is not available, leave the signed copy with the ACO or at the ACO desk. A note shall be made on the inventory stating that the material was permanently removed along with the RFM# of the Receipt For Material.

When the material arrives at the destination, sign and return the Receipt For Material and send it to the DCC at the address in the FROM: block of the Receipt For Material.

4. STORAGE

All classified material must be properly stored in approved storage container and cannot be left unattended at any time.

Network servers may be left running unattended in room 104 only.

At no time is the safe door of room 104 to be left open while the room is unattended. If the room is attended, then the outer door must be kept closed. At the end of the day, both doors must be closed and verified that they are locked.

5. MARKING

All classified material shall be marked in accordance with CHAPTER 4 of the SSOP.

6. NETWORK

We will be using three networks, with no connection to each other. The networks will be as follows:

1. A VAX/VMS network consisting of several VAX and ALPHA servers in room 104 networked together using thin wire Ethernet and several VAX and ALPHA diskless workstations in the front section of room 214 networked together using thin wire Ethernet. Rooms 104 and 214 will be networked together by fiber cable. This network will be run at a security level of Top Secret/Sar.
2. An RDFD peer-to-peer network consisting of several PCs running NT Workstation, networked together using thin wire Ethernet. These PCs will be in the front section of Room 214, and will be used by RDFD personnel. This network will be run at a security level of Secret/Sar.

3. An RDFE PC/Sun peer-to-peer network consisting of 6 PCs running NT Workstation and a Sun Workstation, networked together using RJ-45 twisted pair cables. These PCs will be in the rear section of room 214, and will be used by RDFE personnel. This network will initially be run at a security level of Unclassified, but may in the future be run at a security level of Secret/ Sar.

At no time will the VAX network be left active when there are less than two persons left in the facility who are cleared to the level of the network. Prior to this condition, the network must be disconnected in room 104 by removing power from the Ethernet repeater that feeds room 214.

7. AUDITING

Auditing of VMS network functions shall be accomplished through use of VMS system facilities. Auditing of Windows/NT network functions shall be accomplished through use of Windows/NT system facilities.

1. All log on and log off operations shall be audited.

2. All operations on classified files shall be audited. Classified files shall be maintained on VMS Files-11 or Windows/NT NTFS partitions only.

3. Top Secret material must be brought into accountability immediately.

4. A weekly review of audit trails shall be conducted and the audit file shall be saved on the server and maintained for a period of 12 months.

8. COMPUTERS

8.1 *System Security Profile*

All computers shall have a SAPF 16 on record.

8.2 *Declassification*

Declassification procedures shall be performed on all computers, as per SSOP paragraph 8.403.

8.3 *Repair*

All computer equipment that has been attached to the network, or used for classified processing shall be repaired by appropriately cleared personnel.

9. STORAGE MEDIA

9.1 *Hard Disk*

All hard disks that have been in computers attached to the RDF network shall be classified and marked at the level of the network.

All hard disks outside room 104 must be removed and stored in safes when not in use.

9.2 *Floppy Disk*

Any floppy disk that is used (with the write tab in the *write enable* position) on a classified system assumes the classification of that system.

9.3 *Zip disk*

Due to the lack of a visual write-protect indicator on the zip disk, all zip disk that are used on classified systems shall assume the classification of the system.

9.4 *CDROM*

Any CDROM that is generated using a PC that is classified shall assume the classification of the system unless data has been properly reviewed and verified at lower classification..

9.5 *Magnetic tape*

Any magnetic tape (with the write ring inserted) used on a classified computer shall assume the classification of that system.

9.6 *Other*

No other storage media are authorized for use on the RDF network without specific permission of the RDF network administrator.

10. PRINTERS / PLOTTERS

All printers and plotters shall be checked at the end of each day to verify that all classified documents have been cleared from the machines.

No printers, plotters, or other output devices are to be used on the network if they have ribbons or other media that can maintain an image of classified data.

11. CHECK LIST

At a minimum, the following shall be incorporated into any "end of day" checklist that is used.

Ensure that all classified material is properly stored in GSA approved safe.

Ensure that all printers and plotters are clear of classified documents.

Ensure that all storage media has been removed from all computers and is properly stored.

Ensure network has been disconnected in Room 104.

Ensure that all safes are locked and signed off.

APPENDIX C
RDDR

1. INTRODUCTION

This document outlines the security procedures that are to be followed by all RDDR personnel utilizing the EG&G facility at 821 Grier Drive and is supplementary to the EG&G Security Standard Operating Procedures (SSOP).

It in no way limits the responsibility of all personnel to properly handle, store, and protect classified material.

2. PERSONNEL

Prior to the removal of any Top Secret material, from storage containers, there must be a minimum of two RDDR personnel, who are cleared to the highest classification of the data, present in the facility.

3. INVENTORY

An inventory of all classified material, created by the Document Control Coordinator (DCC), shall be maintained in each safe, kept up to date, and checked weekly.

See attached for a list of responsible individuals.

3.1. *DOCUMENT CONTROL*

All classified material must be checked in through the DCC.

All classified material must have a document control number, assigned by DCC, and then in turn be signed out to the person who will be maintaining the material.

If classified materials are brought into the building during non-duty hours, the materials must be secured and brought into accountability at the earliest possible time prior to use.

3.2 *TEMPORARY REMOVAL*

Classified material leaving the building must have two Receipt For Material forms filled out and one of them signed. The signed copy shall be given to DCC and the other shall accompany the material. If the DCC is not available, leave the signed copy with the ACO or at the ACO desk. An "OUT" card shall be left in place of the material. Blank forms and examples are located in the Document Control Folder of each safe.

When the material is returned, the unsigned copy of the Receipt For Material, that accompanied the material, shall be turned in to DCC and noted that the material has been returned to its original location.

3.3 *PERMANENT REMOVAL*

Classified material leaving the building must have two Receipt For Material forms filled out and one of them signed. The signed copy shall be given to DCC and the other shall accompany the material. If the DCC is not available, leave the signed copy with the ACO or at the ACO desk. A note shall be made on the inventory stating that the material was permanently removed along with the RFM# of the Receipt For Material.

When the material arrives at the destination, sign and return the Receipt For Material and send it to the DCC at the address in the FROM: block of the Receipt For Material.

4. STORAGE

All classified material must be properly stored in approved storage container and cannot be left unattended at any time.

Network servers may be left running unattended in room 104 only.

At no time is the safe door of room 104 to be left open while the room is unattended. If the room is attended, then the outer door must be kept closed. At the end of the day, both doors must be closed and verified that they are locked.

5. MARKING

All classified material shall be marked in accordance with CHAPTER 4 of the SSOP.

6. NETWORK

This network is for engineering development and documentation only. The classification of the network is as briefed. Any non-volatile storage media attached to the network via any method is to be classified at the highest level of the network. The only exceptions are pre-formatted, write protected floppy disks that have data copied to them using the procedures outlined in section 9.2 below.

At no time will the network be left active when there are less than two RDDR personnel left in the facility, who are cleared to the level of the network. Prior to this condition, the network must be disconnected in room 104 by removing power from the Ethernet repeater that feeds room 213.

7. AUDITING

Auditing of VMS network functions shall be accomplished through use of the NT Audit facilities on the NT Server and through IRIX Audit facilities on the IRIX Server, and follow the master AISSP for review requirements.

1. All log on and log off operations shall be audited. This means that the servers must be running prior to operating any comptuers.

2. All operations on classified files shall be audited. Classified files shall be maintained on NTFS partitions only.

3. All print or plot operations involving classified files shall be audited.

4. A weekly review of audit trails shall be conducted and the audit file shall be saved on the server and maintained for a period of 12 months.

8. COMPUTERS

8.1 *System Security Profile*

All computers shall have a SAPF 16 on record.

8.2 *Declassification*

Declassification procedures shall be performed on all computers, as per SSOP paragraph 8.403.

8.3 *Repair*

All computer equipment that has been attached to the network, or used for classified processing shall be repaired by appropriately cleared RDDR personnel.

9. STORAGE MEDIA

9.1 *Hard Disk*

All hard disks that have been in computers attached to the RDDR network shall be classified and marked at the level of the network.

All hard disks outside room 104 must be removed and stored in safes when not in use.

9.2 *Floppy Disk*

Any floppy disk that is formatted on a classified system assumes the classification of that system.

9.3 *Zip disk*

Due to the lack of a visual write-protect indicator on the zip disk, all zip disk that are used on classified systems shall assume the classification of the system.

9.4 *CDROM*

Any CDROM that is generated using a PC that is classified shall assume the classification of the system, unless verified.

9.5 *Magnetic tape*

Any magnetic tape used on a classified computer shall assume the classification of that system, unless verified.

9.6 *Other*

No other storage media are authorized for use on the RDDR network without specific permission of the RDDR network administrator.

10. PRINTERS / PLOTTERS

All printers and plotters shall be checked at the end of each day to verify that all classified documents have been cleared from the machines.

No printers, plotters, or other output devices are to be used on the network if they have ribbons or other media that can maintain an image of classified data.

11. CHECK LIST

At a minimum, the following shall be incorporated into any “end of day” checklist that is used.

Ensure that all classified material is properly stored in GSA approved safe.

Ensure that all printers and plotters are clear of classified documents.

Ensure that all storage media has been removed from all computers and is properly stored.

Physically disconnect network hub in Room 104.

CHAPTER 9. SPECIAL REQUIREMENTS. Not applicable at this time.

CHAPTER 10. INTERNATIONAL SECURITY REQUIREMENTS.

Not applicable at this time.

CHAPTER 11. MISCELLANEOUS INFORMATION

Section 1. COMSEC - STU III TYPE 1 TERMINALS

11-100. General. The provisions of this SOP apply to all persons who use STU III equipment.

11-102. Responsibilities. The STU III Terminal users are responsible for proper use and control of their terminals:

a. Use the secure mode when discussing classified or unclassified national security information.

b. Adhere to the security classification displayed on the STU III terminal for each call.

c. Limit access to a keyed STU III terminal only to persons with a final government security clearance.

d. Control CIKs so that unauthorized/uncleared persons cannot gain access to them.

e. Perform electronic rekeying quarterly or when directed by the COMSEC Custodian or Alternate Custodian(s).

f. Report COMSEC incidents and Insecure Practices to the COMSEC Custodian or Alternate Custodian(s).

11-103. STU III Access Policy.

a. Controlling access to the Type 1 terminal (CCI) to guard against preventable losses to an actual or potential enemy.

b. Persons who do not have a security clearance may use the terminal for unclassified and nonsensitive calls during the day or after hours, as long as the terminal is under the operational control and within view of at least one cleared, authorized person.

c. Persons whose clearance does not meet the level of the keyed terminal are permitted to use the terminal if the terminal is under the operational control and within view of at least one appropriately cleared, authorized person.

11-104. User Identification.

a. Before beginning a secure STU III conversation, the caller must verify that the called party's security clearance meets or exceeds the level of the ensuing

conversation. Voice recognition is an authorized means of verifying a called party's clearance.

b. When two terminals go secure, the STU III digital display automatically show the authentication information of the distant terminal.

c. In calling another party with the STU III, each party's terminal displays the authentication information of the distant terminal. The information displayed only indicates the terminals security capacity, it does not authenticate the security clearance of the person using the terminal.

d. Before beginning a secure STU III conversation, the caller shall insure that called party's security clearance and need-to-know meet or exceed the level of the ensuing conversation.

e. Voice recognition is an authorized means of verifying a called party's clearance.

f. Users shall adhere to the classification level indicated on the terminal display. Due to interoperability among terminals of different classification levels, classification level default to the lowest level, the display may indicated a level less that the actual classification of either terminal's key(s).

11-105. STU III Access Controls.

a. STU IIIs installed and keyed with classified key (CIKs) shall be afforded protection commensurate with the classification of the key in use. When in an area not cleared to the level of the keyed terminal, it must be under the operational control, and within view of, at one appropriately cleared, authorized person (i.e., TOP SECRET cleared if key is TOP SECRET, etc.).

b. STU IIIS in storage shall never be stored in a keyed condition. Prior to placing STU IIIs in storage, the CIKs shall be removed and the internal key storage registers zeroized.

11-106. CIKs For Operational Use. CIKs, when inserted in a Type 1 terminal, gain highest classification level of the associated key and terminal. CIKs not inserted in a STU III terminal, or when in the immediate possession of an authorized user shall be stored as follows:

a. If the CIK is to be stored in the same room as the STU III terminal, it shall be stored in a manner commensurate with the highest classification level of the information the CIK enables the STU III terminal to protect. (TOP SECRET, TOP SECRET storage).

b. If the CIK is to be stored within an EG&G facility, where a STU III has been installed, but in an area apart from the STU III terminal, it shall as a minimum be stored in a locked cabinet or desk, sufficient to reasonably preclude the ability of an unauthorized person to gain access to the CIK and use it in the associated STU III terminal.

c. Any person with unrestricted access to the STU III terminal may retain the operational CIK until it is stored in accordance with a. and b. above.

d. Access to CIKs used operationally is limited to persons that are cleared to the highest level of the associated key and terminal.

All employees granted access to COMSEC information, regardless of form, are responsible for its protection when accountable to them or in their control. They will also be responsible for safeguarding any classified that may come to their knowledge or possession while in the discharge of their assigned duties.

Section 2. EMERGENCY PROCEDURES

11-200. Purpose. To describe procedures for safeguarding classified information during an emergency.

11-201. Actions to be taken.

a. Secure all classified material in authorized security containers or controlled areas.

b. Access Control Officer shall remain with the material if at all possible.

c. Notify, or have someone notify, the FSO for a determination of actions to be taken.

c. The FSO will request assistance as may be deemed necessary, from civil authorities including local, state, or federal law enforcement agencies.

d. If evacuation was necessary, storage containers and controlled areas will be examined upon return to determine whether classified material has been compromised or if any classified material is missing. If appropriate, a report shall be submitted.

e. Any emergency that would inhibit or prevent the proper safeguarding of classified material will be reported, by the quickest means available, to the CSO and the Contracting Officer by the FSO.

e. Legal action may also be taken, such as a court restraining order, or injunction against interference of our property rights or the discharge of contractual obligations to safeguard classified material as deemed necessary.

Section 3. Operations Security (OPSEC).

11-300. OPSEC requirements will be in accordance with the DD254. OPSEC briefings will include:

a. Designated essential elements of friendly information (EEFI).
b. OPSEC lessons learned and the OPSEC role.
c. Common OPSEC vulnerabilities.
d. Significance of unclassified data.
e. Tactical deception.
f. New lessons learned.

The Automated Information System Standard Procedures dated 31 March 2000 is approved in its entirety.

Approved: _____
Bernard VanderWeele
Security Manager/FSO

Approved: _____
Gary H. Fitzgerald
President

Approved: _____
Roger Lackens
PSO

SOP DISTRIBUTION LIST

4/11/00
Bernie VanderWeele
Security Office
2920 Green Valley Parkway
900 A Grier
Gary Fitzgerald