**Standard Practices**

**and Procedures for**

**Safeguarding**

**Classified Material**

**April 2024**



**Gemini Technologies, Inc.**

**2153 Almshouse Rd.**

**Jamison, PA 18929**

**STANDARD PRACTICES & PROCEDURES**

**FOR SAFEGUARDING**

**CLASSIFIED MATERIAL**

Prepared for:

Defense Counterintelligence and Security Agency

Industrial Security, FO (S11PP)

2 Industrial Plaza, Suite 510

Philadelphia, PA 19113-1514

In Accordance with:

DoD 5220.22-M  
with Periodic Updates

Updated by:

Amy Tarara Taber

Facility Security Officer

Submitted by:



(4NQY1)

**PREFACE**

Gemini Technologies, Inc. (Gemini) maintains cleared facilities at the following locations:

Corporate Headquarters

2153 Almshouse Rd,

Jamison, PA 18929

Facility Security Officer: Amy Tarara Taber

Assistant FSO: Robin Taber, President

As Gemini grows and expands each facility will be required to submit a Standard Practice Procedures (SPP) to the Defense Counterintelligence and Security Agency (DCSA) in connection with its facility clearance.

**TABLE OF CONTENTS**

[1. SECRECY AGREEMENT 1](#_Toc164752969)

[2. GENERAL 1](#_Toc164752970)

[2.1. MISCELLANEOUS 1](#_Toc164752971)

[2.1.1. Industrial Security Check 2](#_Toc164752972)

[2.1.2. Self-Inspections 2](#_Toc164752973)

[2.1.3. Standard Practice Procedure 2](#_Toc164752974)

[2.1.4. Operations Security (OPSEC) 2](#_Toc164752975)

[2.1.5. Advertisements/Security Requirements 2](#_Toc164752976)

[3. EMERGENCY PRODCEDURES 3](#_Toc164752977)

[3.1. PHYSICAL EMERGENCY 3](#_Toc164752978)

[3.2. DEFENSE HOTLINE 4](#_Toc164752979)

[4. SECURITY CLEARANCES 5](#_Toc164752980)

[4.1. FACILITY CLEARANCES 5](#_Toc164752981)

[4.2. PERSONNEL SECURITY CLEARANCES 5](#_Toc164752982)

[4.2.1. Pre-employment Clearance Action 6](#_Toc164752983)

[4.2.2. Completing National Background Investigation Services (NBIS) Electronic Questionnaire for Investigation 6](#_Toc164752984)

[4.2.3. Record Maintenance 6](#_Toc164752985)

[5. SECURITY EDUCATION 7](#_Toc164752986)

[5.1. Basics of Employee Security Education 7](#_Toc164752987)

[5.2. Continuing Employee Security Education 9](#_Toc164752988)

[6. ASSIGNMENT OF RESPONSIBLIITIES 10](#_Toc164752989)

[6.1. KEY PERSONNEL/MANAGEMENT 10](#_Toc164752990)

[6.2. FACILITY SECURITY OFFICER 10](#_Toc164752991)

[6.3. PROJECT MANAGER/SUPERVISORS 11](#_Toc164752992)

[6.4. INFORMATION TECHNOLOGIST (IT) 11](#_Toc164752993)

[6.5. EMPLOYEE 11](#_Toc164752994)

[6.6. AUTOMATED INFORMATION SYSTEM SECURITY PERSONNEL 12](#_Toc164752995)

[6.6.1. Automated Information System Security Supervisor 12](#_Toc164752996)

[6.6.2. System Security Custodian 12](#_Toc164752997)

[7. SUBCONTRACTORS, VENDORS, AND SUPPLIERS 12](#_Toc164752998)

[7.1. GENERAL 12](#_Toc164752999)

[7.2. DD 254 - CONTRACT SECURITY CLASSIFICATION SPECIFICATION 13](#_Toc164753000)

[8. CONSULTANTS 13](#_Toc164753001)

[9. CLASSIFIED VISITS & TRAVEL 13](#_Toc164753002)

[9.1. CLEARED EMPLOYEES TO OTHER FACILITIES OR GOVERNMENT ACENCY FACILITIES 13](#_Toc164753003)

[9.2. FOREIGN TRAVEL AND ATTENDANCE AT MEETINGS 14](#_Toc164753004)

[9.3. VISITS TO GEMINI BY EMPLOYEES OF OTHER FACILITIES OR GOVERNMENT AGENCIES 14](#_Toc164753005)

[9.4. CLASSIFIED MATERIAL IN CONNECTION WITH VISITS 15](#_Toc164753006)

[10. HANDLING CLASSIFIED MATERIAL 15](#_Toc164753007)

[10.1. HANDLING CLASSFIED MAIL 15](#_Toc164753008)

[10.1.1. Accepting Registered, Certified Or U.S. Express Mail 15](#_Toc164753009)

[10.1.2. Document Accountability Form 16](#_Toc164753010)

[10.1.3. Classified Mail – Outgoing 16](#_Toc164753011)

[10.2. TRANSMISSION OF CLASSIFIED MATERIAL OUTSIDE A FACILITY 17](#_Toc164753012)

[10.2.1. Preparation For Transmission – Outside Gemini 17](#_Toc164753013)

[10.2.2. Addressing Mail or Shipment of Classified Material 17](#_Toc164753014)

[10.2.3. Use Of FedEx or Other Approved Couriers For Overnight Transmission Of Classified Information Within The Continental U.S. 17](#_Toc164753015)

[10.2.4. Receipt of FedEx or other Courier Addressed to “Security Office” or “FSO” 19](#_Toc164753016)

[10.2.5. Transmission Outside the U.S., Puerto Rico, or U.S. Possession or Trust Territory 20](#_Toc164753017)

[10.2.6. Couriers, Hand-Carriers and Escorts 21](#_Toc164753018)

[10.3. HAND CARRYING OF CLASSIFIED DOCUMENTS AND HARDWARE 21](#_Toc164753019)

[10.4. HANDLING MATERIAL WITHIN A FACILITY 22](#_Toc164753020)

[10.4.1. TRANSMISSION OF MATERIAL WITHIN A FACILITY 22](#_Toc164753021)

[10.4.2. Reproduction 22](#_Toc164753022)

[10.4.3. Safeguards During Use 22](#_Toc164753023)

[10.4.4. Destruction 23](#_Toc164753024)

[11. MARKING CLASSIFIED MATERIAL 25](#_Toc164753025)

[11.1. GENERAL 25](#_Toc164753026)

[11.2. CLASSIFICATION ROLES AND RESPONSIBILITIES 25](#_Toc164753027)

[11.2.1. Security Classification Guidance 25](#_Toc164753028)

[11.2.2. Roles and responsibilities 26](#_Toc164753029)

[11.3. MARKINGS 26](#_Toc164753030)

[11.3.1. Identification Markings 26](#_Toc164753031)

[11.3.2. Initial Markings 26](#_Toc164753032)

[11.3.3. Portion Markings 26](#_Toc164753033)

[11.3.4. Additional Markings 28](#_Toc164753034)

[11.3.5. Derivative classification 28](#_Toc164753035)

[11.3.6. Dates or events carried forward 28](#_Toc164753036)

[11.3.7. Changing classification markings 28](#_Toc164753037)

[11.3.8. Release of declassified information 28](#_Toc164753038)

[11.3.9. Downgrading/declassification and “Classified by” line procedures 28](#_Toc164753039)

[12. SAFEGUARDING CLASSIFIED INFORMATION 29](#_Toc164753040)

[12.1. CONTROL OF AREAS 29](#_Toc164753041)

[12.1.1. GENERAL 29](#_Toc164753042)

[12.1.2. Closed Area 29](#_Toc164753043)

[12.1.3. Restricted Area 29](#_Toc164753044)

[12.2. STORAGE OF CLASSIFIED MATERIAL 30](#_Toc164753045)

[12.2.1. SECRET Material 30](#_Toc164753046)

[12.2.2. CUI Material 31](#_Toc164753047)

[12.3. Digital Documentation Handling 32](#_Toc164753048)

[12.3.1. Transmission of Documentation 32](#_Toc164753049)

[12.3.2. Access Controls and Cybersecurity 32](#_Toc164753050)

[13. SECURITY VIOLATIONS AND INFRACTIONS 32](#_Toc164753051)

[13.1. GENERAL 32](#_Toc164753052)

[13.2. ADMINISTRATIVE MEASURES 33](#_Toc164753053)

[14. REPORTING REQUIREMENTS 33](#_Toc164753054)

[14.1. REPORTS TO THE COGNIZANT SECURITY AGENCY (CSA) 33](#_Toc164753055)

[14.2. REPORTS TO THE FBI 35](#_Toc164753056)

[15. OPERATIONS SECURITY (OPSEC) 35](#_Toc164753057)

[15.1. INSIDER THREATS 36](#_Toc164753058)

[15.1.1. General 37](#_Toc164753059)

[15.1.2. Targeted Individuals 37](#_Toc164753060)

[15.1.3. Threat Intelligence 37](#_Toc164753061)

[15.1.4. Employee Training 37](#_Toc164753062)

[15.1.5. Reporting Insider Threats 37](#_Toc164753063)

[15.2. ANALYSIS OF EXTERNAL THREATS 37](#_Toc164753064)

[15.2.1. Counterintelligence Awareness 38](#_Toc164753065)

[15.2.2. Counterintelligence Objectives 38](#_Toc164753066)

[15.2.3. Protecting the Parts 38](#_Toc164753067)

[15.2.4. Reporting the Threat 39](#_Toc164753068)

# SECRECY AGREEMENT

A substantial part of the work done by Gemini Technologies, Inc. (Gemini) is of military nature and must be entered into with the distinct understanding that all information pertaining to such work must be safeguarded rigidly in accordance with the laws of the United States, and the regulations of the Department of Defense (DoD).

Every employee having access to any material classified as TOP SECRET, SECRET, or CUI is forbidden legally to discuss that information except to the extent necessary in the performance of work as assigned by the company. The disclosure by an employee of any such information to any person not entitled to receive it, or failure by an employee to safeguard all TOP SECRET, SECRET, and CUI information in the employee’s possession may subject the employee to criminal prosecution.

It is an offense punishable by fine, imprisonment, or both for any person who has possession of or access to any document, sketch, photograph, model, map, or appliance relating to national defense to transmit (or attempt to transmit) the same to any person not entitled to receive it. Criminal prosecution also applies if an employee, through gross negligence, permits such material to fall into unauthorized hands or to be lost, stolen, or destroyed. If any employee has knowledge of the loss, theft, or destruction of such material, they are required to report the happening to their superior and/or the location’s Facility Security Officer (FSO) or assistants.

It is also a punishable offense to produce without proper authority, any photograph, sketch, drawing, or other graphic representation of any TOP SECRET, SECRET, or CUI equipment, tools, documents, plans or installations, of any establishment engaged in the development or manufacture of classified material.

Gemini has entered into a contractual agreement with the Department of Defense in that classified information may be made available to Gemini only as long as all of the required standards and regulations are observed in the proper use and safeguarding of this information.

The FSO is responsible for ensuring that our company adheres to the requirements of the National Industrial Security Program (NISP).

# GENERAL

## MISCELLANEOUS

Questions regarding security procedures not covered in this manual shall be referred to the FSO. Further details of all procedures may be found in the National Industrial Security Program Operating Manual (NISPOM) DoD Federal Register Vol. 85, No. 245, 32 CFR Part 117, dated Monday, December 21, 2020 ([eCFR :: 32 CFR Part 117 -- National Industrial Security Program Operating Manual (NISPOM)](https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117)), with periodic updates. Copies are available from the FSO.

On a recurring basis all cleared personnel shall be reminded of their continuing responsibility for safeguarding classified information. Each cleared employee shall be made aware of the security procedures that pertain to the employee’s particular work assignment, and any deficiencies resulting from inspections from the Cognizant Security Office (CSO) that require corrective action on the part of the employee.

Access to a copy of this SPP is provided to all cleared employees

Employees who fail to observe the requirements of this manual will be notified by means of a ‘‘Notice of Security Deficiency’’ forwarded to the employee’s immediate Supervisor.

**A clearance is not an automatic authorization for access to classified information. The ‘‘need-to-know’’ must be established before releasing classified information to visitors as well as other Gemini employees.**

### Industrial Security Check

Gemini’s Jamison, PA facility has a SECRET facility clearance without retention (storage) capabilities, Government inspections / reviews take place every 12 to 18 months.

### Self-Inspections

The FSO or designee will conduct a self-inspection at least once a year. This inspection will consist of an audit of each facility’s operation according to the requirements of the NISPOM, utilizing the Self-Inspection Job Aid, and will include all elements normally inspected by DCSA. Deficiencies will be noted and corrected as soon as possible. A record of these self-inspections will be uploaded in digital form as required to the DCSA National Industrial Security System (NISS) online application, and maintained to be made available for review by DCSA during the next regularly scheduled inspection.

### Standard Practice Procedure

Geminishares Standard Practice and Procedure (SPP) application throughout the organization, which will be adapted as necessary, to apply to each specific location, as the corporation grows. A copy of the SPP is then furnished to each CSO for approval. Upon notification from the CSO the SPP will be made available to all cleared personnel. The SPP will also be revised as necessary, to implement revisions applicable to Gemini’s operation within 6 months after notification of changes to national security policy and requirements.

### Operations Security (OPSEC)

Although not a component of the National Industrial Security Program (NISP), the DoD Operations Security Program (OPSEC) is discussed in this manual in order to provide Gemini personnel participating in the DISP with advice and guidance concerning OPSEC in the event they become involved with this program via User Agency (UA) imposed OPSEC contractual requirements. The DoD OPSEC program is applicable only to defense contractors participating in the DISP when the contractor UA determines that OPSEC measures are essential to protect classified information for specific classified contracts.

### Advertisements/Security Requirements

The fact that a contractor has qualified for or has been granted a facility clearance (FCL) it should not be used for advertising or promotional purposes. All newspaper advertisements must be approved, by the FSO, **BEFORE** the advertisement is placed. The advertisement **CAN** contain the following clause if the position requires a security clearance:

|  |  |  |
| --- | --- | --- |
|  | ***‘‘Applicants selected will be subjected to a government security investigation and must meet eligibility requirements for access to classified information.’’*** |  |

You **MUST NOT**, however, ask the applicant if *they* are *a United States citizen*.

The interviewer might find it necessary to screen applicants before calling them in for an interview. Both the DCSA and the Human Rights Office have agreed that we ***can discuss*** the following items with a potential candidate:

*For Example:*

Entry Level Programmer

Salary Range: $20,000 - $22,000

Qualifications: Must know ADA and C

Experience with dBase, Excel, FoxPro, and Windows

Applicant must meet security eligibility requirements

This will hopefully eliminate recruiting individuals who are not eligible to receive a security clearance (other than a Limited Access Authorization) when one will be required. It **IS NOT** Gemini’s policy to tell anyone that he or she must be a United States citizen. Gemini is an equal opportunity employer.

# EMERGENCY PRODCEDURES

|  |  |  |
| --- | --- | --- |
|  | ***The Emergency Procedures section does not currently apply to Gemini. Gemini is not currently a “retaining” facility and therefore does not have classified material stored in its facility(ies). This section has been included as a reference and training guide for future implementation when the time arises*.** |  |

## PHYSICAL EMERGENCY

In the event of an emergency, such as a natural disaster or any civil disturbance, bomb threat or the like, the following emergency procedures will be followed:

1. A state of emergency may be declared by one of the following in this order of preference: Robin Taber *(President),* Paulina Anderson-Dinitz *(COO),* Amy Tarara Taber *(FSO).*

2. The FSO will immediately notify the CSO by telephone of the imminence of any situation that could present a threat to classified information.

The Cognizant Security Office is:

Defense Counterintelligence and Security Agency

Industrial Security Field Office (S11PP)

2 International Plaza, Suite 510

Philadelphia, PA 19113-1514

E-mail: [dss.dss-northern.dss-isfo.mbx.philadelphia-field-office@mail.mil](mailto:dss.dss-northern.dss-isfo.mbx.philadelphia-field-office@mail.mil%20)

Telephone: (610) 537-1060

Unclassified Fax: (610) 595-1874

***Code S1411*** for Facility Clearance, KMPs, and Reports

***Code S14PP*** for Inspection, SPP, and Guidance

The Warwick Township Police Department, and/or Pennsylvania State Police will be notified by the FSO.

Warwick Township Police Department Pennsylvania State Police, Troop M, Bethlehem

(215) 343-8165 (610) 861-2026

1. After issuing the above notifications, the FSO will conduct an immediate inventory of all classified material and secure such in its assigned container, or instruct the possessing employee to maintain custodial responsibility of the material until it can be put into an approved container and properly secured. *Gemini is currently a non-retaining facility.*
2. Each employee is responsible for protecting any classified material is in their possession. If time permits, it shall be placed in the proper container and secured. If time does not permit, the employee shall carry the material with them with the proper cover. It then becomes their responsibility to safeguard it properly until the material can be placed in an appropriate container.

After the emergency is over DCSA will be notified by a classified report, if appropriate, if classified information is believed to have been compromised or is missing.

## DEFENSE HOTLINE

The following address and phone number are included here to provide Gemini employees with and unconstrained avenue to report any known or suspected instances of fraud, waste, and/security irregularities and infractions concerning defense contracts, programs, or projects. The Defense Hotline is organized and administered by the Office of the Inspector General, DoD. This office initiates investigative action regarding information received through the Defense Hotline system and has primary responsibility for ensuring the confidentiality of all system users.

A digital report can be filed online: <https://www.dodig.mil/Components/Administrative-Investigations/DoD-Hotline/>

To render a report by phone or in writing, the address is as follows:

Defense Hotline

The Pentagon

Washington, DC 20301-1900

(800) 424-9098

# SECURITY CLEARANCES

## FACILITY CLEARANCES

A facility clearance (FCL) is an administrative determination that a facility is eligible, from a security viewpoint, for access to classified information. In Gemini’s case, the User Agency determined that Gemini’s Jamison, PA, facility needed clearance to a SECRET level. In order to be eligible for custody (possession) of classified material to the SECRET level, in addition to an FCL, Gemini must show that it can comply with the proper storage capability requirements (when the time arises) to the CSO. *Gemini is currently a non-retaining facility.*

## PERSONNEL SECURITY CLEARANCES

Security clearances are granted to both facilities and personnel. Clearances are granted at the SECRET and TOP SECRET levels depending on the level of information to which access is required. An individual may be granted a clearance at a lower level than the facility but may never have a clearance level higher than the facility’s. *Gemini is currently cleared to the Secret level.*

Requests for Personnel Security Clearance (PCL’s) will be processed through the FSO from the information obtained from the employee and the employee’s supervisor.

Certain personnel, such as the officers and the FSO of the company, are required to be cleared as part of the facility clearance process. Other than these personnel, only employees whose work requires them to have access to classified information will be processed for a security clearance.

When an individual no longer needs access to classified information, his or her clearance must be suspended. PCLs, which have been suspended, can be reinstated by the FSO, or designee, by updating the information in the Defense Information System for Security (DISS) Joint Verification System (JVS) provided:

1. No more than 24 months has lapsed since the date of suspension of clearance.

2. There is no adverse information.

3. The most recent investigation has not exceeded 10 years for Secret, 5 years for Top Secret.

4. Must meet or exceed the scope of the investigation required for the level of PCL that is to be reinstated or granted.

See the FSO for details. Supervisors are responsible for assisting the FSO in keeping the number of PCLs to a minimum.

**An employee may not have access to classified information until receipt of at least an Interim Authorization with Limited Access Authorization (LAA), per paragraph 2-210 of the NISPOM, has been briefed by the FSO, and signed an SF-312 Classified Information Nondisclosure Agreement (**Figure 1. SF-312 (Page 1) **and** Figure 2. SF-312 (Page 2)**).**

### Pre-employment Clearance Action

Pre-employment clearance action should not be initiated unless the recruitment is for a specific position that will require access to classified information. Wording for employment adver­tisement should read:

|  |  |  |
| --- | --- | --- |
|  | ***‘‘Applicants selected will be subjected to a government security investigation and must meet eligibility requirements for access to classified information.’’*** |  |

The completed PCL application may be submitted to the CSA prior to the date of employment, provided that a written commitment for employment has been made by Gemini and the Contracting Agency with a fixed date for employment within the ensuing 180 days and the candidate has accepted the employment offer in writing.

### Completing National Background Investigation Services (NBIS) Electronic Questionnaire for Investigation

The FSO will give the employee instructions on how to fill out and access NBIS eApp, the digital submission of form SF86, on the employee’s computer. The applicant should complete the eApp questionnaire according to the instructions within 90 days. The privacy section can be completed in private by following the instructions on the NBIS access page (<https://www.dvidshub.net/video/847850/eapp> ).

The FSO is denied access to this information; only when the subject submits their application for review can the FSO see any of the eApp information. When completed, the draft eApp application will be made available for the FSO to review for *compliance and completeness only*. During this process, the FSO will instruct the employee on the procedure to obtain digital fingerprints from an approved agency. Once the fingerprint digital file has been obtained, the FSO will upload the appropriate biometric data to the Secure Web Fingerprint Transmission (SWIFT) page (<https://swft.nbis.mil/default.aspx>). Once the NISS eApp is deemed complete and approved by the FSO, the application is then submitted to DCSA through the NBIS FSO page. The individual being processed for a PCL must produce acceptable proof of U.S. citizenship as required by Paragraph 2-207 of the NISPOM.

NOTE: As of October 2023, there is a “swivel-chair” requirement to enter subjects into DISS JVS as well as NBIS. As the online NISS eAPP procedures are updated, the SPP will be updated to reflect changes.

Requests for clearances of key management personnel (KMP) (formerly owners, officers, directors, partners, regents, trustees, or executive personnel [OODEPs]) such as the FSO must be submitted through the CSO.

### Record Maintenance

DCSA notifies the company when a PCL is issued via DISS. All eApp information is stored digitally within the NISS subject database, and a pdf version can be accessed on the FSO portal. Unless terminated, suspended, or revoked by the Government, the subject’s access to classified material remains effective as long as the subject is employed by Gemini and clearances are renewed on a regular basis per the NISPOM, or the subject can be enrolled in Continuous Evaluation in the JVS system to automatically renew.

The FSO will maintain a current list of cleared employees located at both cleared and uncleared facilities. The list will include names of cleared employees and the address of the facility to which they are assigned.

# SECURITY EDUCATION

## Basics of Employee Security Education

The security education program is designed to acquaint all employees with the principles of security and to emphasize the employee’s continuing individual responsibilities to protect classified information.

Upon joining the company, each employee will be given an initial security briefing as part of onboarding consisting of an overview of the industrial security program, classification definitions, document handling, and insider threats. Gemini’s satellite offices will be briefed digitally and recurring briefings will be done bi-annually, at the minimum, by the FSO or designee of the supporting cleared facility.

When employees receive their security clearances, they will then be given thorough briefings as to their individual security responsibilities, with emphasis on those security procedures which directly affect their work tasks. The briefing will include, but not limited to the following:

1. Threat Awareness
2. Defensive Security
3. Overview of the Security Classification System
4. Employee reporting obligations and requirements
   1. Change of name
   2. Change of marital status
   3. Change in citizenship
   4. Foreign travel/trips out of the country *(vacation or business)*
5. Security procedures and duties applicable to the employee’s job

Following this briefing, the employee shall be required to execute the *‘‘Classified Information Nondisclosure Agreement’’,* Standard Form 312 (SF312) *(see Figure 5-1)*. The employee’s signature shall be witnessed by his/her supervisor or by another designated employee. Both signatures must bear the same date. The SF 312 must also be signed and accepted by the FSO who has been specifically delegated authority to accept, on behalf of the U.S. government. The SF 312 is uploaded to DISS JVS, with a copy retained in the employee’s security file.

The FSO is required to submit a report immediately to the CSA when an employee refuses to execute the SF 312.



Figure 1. SF-312 (Page 1)

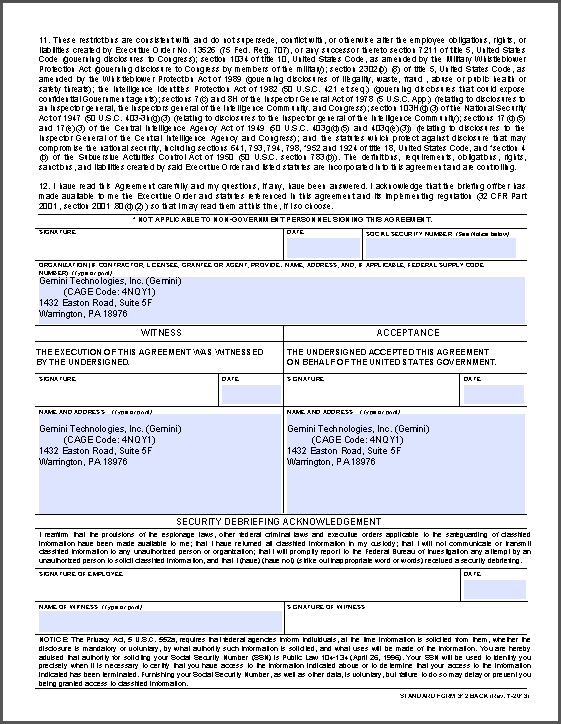


Figure 2. SF-312 (Page 2)

## Continuing Employee Security Education

Employees shall be periodically reminded of their individual security responsibilities through oral reminders and the circulation of written security awareness material.

Per the NISPOM, all employees will receive annual refresher training, and each employee will provide the FSO a signed acknowledgement form of receipt and review of the refresher briefing.

At a minimum, refresher briefings shall reinforce the information provided during the initial briefing and inform employees of appropriate changes in security regulations. This requirement can be satisfied by the use of audio/video materials and by issuing written materials, or e-mail, on a regular basis.

Additionally, pertinent security threats will be communicated to all employees upon receiving the information from cleared DCSA briefings, as appropriate and applicable. These briefing, typically distributed quarterly, disseminate the most current security information pertinent to the post prevalent threats at the time.

# ASSIGNMENT OF RESPONSIBLIITIES

The following defines the Roles and responsibilities assigned to individuals within Gemini.

## KEY PERSONNEL/MANAGEMENT

Key Management Personnel includes the President, Chief Financial Officer (CFO), and Chief Operating Officer (COO). These roles support and enable the FSO to process, disseminate and monitor the security of the facility and the personnel.

The President and CFO ensure that all contractual security obligations are documented and noted for implementation for potential and awarded work.

The COO interprets the DD 254 - Security Classification Specification attached to contractsand ensures clearance requirements tied to contractual performance are communicated to Project Managers.

All Key Personnel advise the FSO to initiate clearance applications as needed for new hires.

## FACILITY SECURITY OFFICER

The Facility Security Officer shall:

1. Have overall responsibility for all matters pertaining to government security procedures.

2. Establish security policy compatible with the policies and standards set by management, set up operating standards, and prescribe the procedures necessary to safeguard classified material from unauthorized access.

3. Obtain retention authority for classified documents, when required, and furnish the Contract Administrator with results of retention requests.

4. Supervise document control, including the creation, maintenance, retention, and disposition of records necessary for the security program.

5. Supervise the disposition of classified material associated with pre-contract and end-of-contract activity, and other material as required.

6. Supervise the transmission and release of classified material outside the facility.

7. Keep informed of government security directives and disseminate information within the company, conducting group briefing sessions when necessary.

8. Conduct periodic security inspections as necessary to ensure compliance with security regulations.

9. Brief employees who plan to attend conferences, seminars, etc., including foreign travel, on the proper handling of classified information. A debriefing is also conducted after foreign travel.

10. Ensure that adequate classification guidance is received, understood, applied, and challenged, if necessary; ensure that documents are accurately marked by appropriate personnel, and that the documents are downgraded and declassified as authorized.

11. Preclude access to classified information if a clearance is denied, suspended, or revoked. Evaluate assigned duties to determine whether reassignment is necessary.

12. Ensure that classified material is properly controlled during use and that classified visits to the facility are properly arranged and conducted.

13. Limit and control the reproduction of classified material.

## PROJECT MANAGER/SUPERVISORS

The Project Manager or Supervisor, whose signature or other form of approval is required before a document is transmitted outside the facility, determines that the necessity, currency, and accuracy of the security classification markings applied to the document are in compliance with the DD Form 254 issued with each contract/subcontract/task.

Supervising personnel should maintain vigilance within the work area to assure compliance with security regulations. The supervisor determines the “need to know” when granting individuals access to classified material and advises the FSO of the existence of any information concerning any employee, cleared or in the process of being cleared, that indicates that such access to classified information may be questionable or not in the interest of national security.

When appropriate, the Project Manager advises employees, on a need-to-know basis, how to apply the appropriate classification markings on generated classified material.

Management shall also ensure that he/she completes the required security training.

## INFORMATION TECHNOLOGIST (IT)

Due to the increased demand in digital communication, document sharing and system access, the IT hold a critical role in monitoring and addressing information security issues in compliance with NIST 800-171.

Working with the FSO, Project Managers and Supervisors, as well as interfacing with employees, IT implements local digital accesses not related to DoD systems to enable cleared employees to work safely.

## EMPLOYEE

Individual employees should observe at all times the letter and spirit of this manual and any other instructions issued by the FSO to safeguard classified information. Employees who copy or extract classified information from another document, or who reproduce or translate an entire document are aware of their responsibilities for marking the documents appropriately.

Employees are responsible for the procedures as outlined in this SPP, including sections on Handling Classified Material; Marking Classified Material; Visitor Control, Subcontractors, Vendors, and Suppliers; Consultants; and Gemini’s Security System.

The employee also realizes it is his/her moral and legal obligation to report to the FSO any violations of security, either actual or suspected, or any questionable contact with nationals or representatives of other countries. Questionable contact in this regard is any personal exchange, encounter, or relationship that is determined to consist of an actual, probable, or possible hostile intelligence collection effort.

## AUTOMATED INFORMATION SYSTEM SECURITY PERSONNEL

### Automated Information System Security Supervisor

The AIS Security Supervisor develops the procedures for programming and software issues and readies the computer for use with classified information. The responsibilities of the AIS Security Supervisor are enumerated in the *Automated Information System Standard Practice Procedure*, which is a stand-alone companion manual to this SPP. A copy of this manual is issued to cleared personnel on an as-needed basis and can be obtained from the FSO. *Gemini currently does not utilize an AIS*.

### System Security Custodian

This is a term to define employees who are users of the AIS. They must be properly cleared and have a need-to-know in order to be allowed access to the room or use the computer(s) when they are in use for classified work.

# SUBCONTRACTORS, VENDORS, AND SUPPLIERS

## GENERAL

Before requesting a bid from a subcontractor, vendor, or supplier on a classified procurement, it is most important to establish that the company concerned has a facility clearance and storage capability, if needed, to the level required to perform the subcontract, if awarded.

Verifications of a vendor’s facility clearance and/or safeguarding capabilities may be requested from the NISS via the Internet or letter, and will remain valid for three calendar years unless superseded in writing by the NISS. The FSO will process the request for this information and notify the requesting department of the results of the inquiry.

**Under no circumstances shall classified work be sublet without certifying the subcontractor’s facility clearance through the Facility Security Officer.**

If a prospective subcontractor does not have the appropriate facility clearance or safeguarding capability the FSO, after corporate approval, may request the subcontractor’s CSA to initiate the necessary action (see paragraph 7-101b(2) in the NISPOM for specifics).

## DD 254 - CONTRACT SECURITY CLASSIFICATION SPECIFICATION

When a quote on a classified contract is to be solicited from a subcontractor, vendor or supplier, it must be accompanied by a DD 254 - *Contract Security Classification Specification*. This form is prepared and distributed by the Contracts Department and the Facility Security Officerupon receipt of the necessary information from the DD 254issued with the prime contract, indicating the classification of the material involved in the performance of the subcontract only.

*Approval of the Contracting Officer is required before submitting the form to the prospective subcontractor or vendor.*

After selection of a subcontractor or vendor, the FSO must be informed promptly by the procuring department. A new DD 254 will be prepared and submitted to the Contracting Officer for approval and distribution as indicated on page 2 of the DD 254.

A revised DD 254 shall be issued as necessary during the lifetime of the subcontract when security requirements change. A final DD 254 for a subcontract shall be issued by the prime contractor in accordance with paragraph 7-103 of the NISPOM.

**NOTE: The above requirements apply also to contract labor (secretarial, janitorial, etc.) employed to work in classified areas or on classified material.**

# CONSULTANTS

A consultant is an individual under contract to provide professional or technical assistance to a contractor or Government Contracting Activity (GCA) in a capacity requiring access to classified information. The consultant shall not possess classified material off the premises of the using (hiring) contractor or GCA except in connection with authorized visits. The consultant and the using contractor or GCA shall jointly execute a consultant certificate setting forth respective security responsibilities. The using contractor or GCA shall be the consumer of the services offered by the consultant it sponsors for a PCL. For security administration purposes, the consultant shall be considered an employee of the hiring contractor or GCA. The CSO shall be contacted regarding security procedures to be followed should it become necessary for a consultant to have custody of classified information at the consultant’s place of business.

# CLASSIFIED VISITS & TRAVEL

## CLEARED EMPLOYEES TO OTHER FACILITIES OR GOVERNMENT ACENCY FACILITIES

When it becomes necessary for employees of Gemini to visit other cleared contractors or Government agencies and access to classified information is anticipated, employees must notify the FSO and provide the contractor or agency to be visited the contractor or agency’s CAGE Code or SMO, the time and duration of visit, the reason for the visit, security classification of the visit, if applicable, the person to be contacted, and the POC for the facility visit approval if possible. To avoid a delay in the processing or rejection of visit requests, care should be exercised in using nicknames, abbreviations and acronyms that may be unfamiliar to the recipient. Where repeated, use of short terms is desirable for brevity, with an explanation provided.

**All classified visits require 48hour advance notification to, and approval from, the place being visited**.

Ample time must be allowed to permit the visit authorization request to be prepared, submitted via JVS to the contractor/agency, and processed by their visitor control.

## FOREIGN TRAVEL AND ATTENDANCE AT MEETINGS

Any cleared employee who intends to travel to or through a foreign country (vacation or work related), or attend an international meeting, regardless of geographic location, at which it is anticipated that representatives of foreign countries will also attend ***must notify the Facility Security Officer before leaving on travel.*** The employee must complete a Foreign Travel Briefing form with the details of their travel, including dates of travel, mode of travel, destination (s) with addresses, an emergency contact and any anticipated foreign national contacts. The FSO will brief the employee regarding his/her responsibilities, and will update the subject’s foreign travel information in DISS JVS.

Upon completion of foreign travel or attendance at an international meeting at which representatives of a foreign country participated in or attended, the employee will complete a Foreign Travel Debriefing form, compliant with update SEAD 3 requirements. They will inform the FSO as to whether or not there had been a possible security compromise. The FSO will file a report with DCSAOC or the appropriate agency.

## VISITS TO GEMINI BY EMPLOYEES OF OTHER FACILITIES OR GOVERNMENT AGENCIES

***This section*** ***currently does not apply to Gemini. Gemini is not currently a “retaining” facility and therefore does not have approval for retention of classified material or the ability to sponsor classified meetings. It has been included as a reference and training guide for future implementation when the time arises*.**

Requests from other cleared facilities or government agencies for visits to Gemini by their per­sonnel requiring access to classified information will be directed to the Security Officer.

The person to be visited will be notified, and the visitor’s level of security clearance will be validated.

If classified material is to be brought to or removed from Gemini, the facility clearance of the visitor’s place of business will be verified by the FSO by checking the NISS website before any classified material is prepared for shipment.

It is the responsibility of the receptionist to identify visitors and require them to sign the visitor logbook. A North Atlantic Treaty Organization (NATO) visitor’s logbook for all NATO visitors is also kept at the receptionist’s desk. The Security Office/FSO will maintain a file of all cleared visitors.

Authorized visitors who will require access to classified information will be escorted at all times by a Gemini employee cleared, with a need-to-know, to a level at least equal to the classification of the material to which the visitor will have access. The escort shall be responsible for denying the visitor access to any classified information for which he/she is not authorized.

Foreign nationals or representatives of foreign governments **MUST BE ESCORTED AT ALL TIMES.** Other visitors who do not require access to classified information need not be escorted, except under extreme situations. However, all Gemini employees must exercise caution to deny such visitors access to classified information.

## CLASSIFIED MATERIAL IN CONNECTION WITH VISITS

When classified material is required on a visit, the material should be mailed in advance, according to standard procedures, to the facility to be visited. It should be addressed to the Gemini employee, with instructions to be held for his/her arrival. This method also should be used for the return of classified material. If time does not permit mailing, the Gemini employee may be authorized to hand-carry the classified material, provided they will arrive at the Gemini or other designated cleared facility, before the end of normal working hours for that day.

An inventory of all classified material leaving Gemini must be conducted before departure. This inventory, which applies to material hand carried as well as forwarded in any other manner, is recorded on an In-Transit Receipt for Classified Material. Upon the employee’s return from the visit, another inventory will be made of the material for which he/she is responsible. If classified material is not returned to Gemini, a signed receipt must be obtained from the authorized person at the receiving facility and the transaction entered into the document accountability records.

# HANDLING CLASSIFIED MATERIAL

***The procedures in section 11.1 through 11.2 do not currently apply to Gemini. Gemini currently is not a “retaining” facility and therefore does not have an approval for retention of classified material. These sections have been included as a reference and training guide for future implementation when the time arises***.

The following information pertains to the physical handling and storage of classified information. The initial sections

## HANDLING CLASSFIED MAIL

### Accepting Registered, Certified Or U.S. Express Mail

Incoming material is considered classified until opened. This material will not be accepted unless Signed for by the Facility Security Officer or designated authorized personnel.

All classified mail is then entered into Document Control records, and the appropriately cleared addressee is notified of receipt. Receipts for incoming classified mail will be signed by the FSO, or a designated alternate, at the time of delivery; the original is returned to the sender, and a copy is retained by the Security Office for two years.

### Document Accountability Form

This form (Figure 3) is to be completed by the FSO each time a classified document is received and placed into the classified container; transmitted out of the facility; or when additional copies are made.

|  |
| --- |
| Figure 3. Document Accountability Log |

### Classified Mail – Outgoing

All classified mail leaving Gemini, including hand-carried documents, must be brought to the Security Officer for authorization to release **BEFORE** transmission. Outgoing classified material must also be recorded in the Security Office. A Classified Document Receipt) for all accountable classified material will then be prepared for shipment.

A copy of the receipt will be kept as a record of transmission (mailed or hand-carried) until a signed receipt is received. If a signed receipt is not received within 30 days, follow-up procedures will commence. In the event a signed receipt is not obtained within 90 days, DCSA will be notified. Returned signed receipts for outgoing material will also be retained by the Security Office for a minimum of 2 years.

SECRET documents, including working papers, shall be entered into the control station account­ability when the document is:

* A completed document in excess of 180 days from the date of completion;
* Reproduced for internal purposes;
* Retained as a partially completed document or discontinuance of the work; or
* Transmitted, regardless of the stage of development, outside of the facility on a temporary or permanent basis.

## TRANSMISSION OF CLASSIFIED MATERIAL OUTSIDE A FACILITY

### Preparation For Transmission – Outside Gemini

Classified information in physical/paper form 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 the sender and the addressee. The outer cover shall be sealed and addressed with no identification of the classification or its contents. A receipt shall be attached to or enclosed in the inner cover, except that CUI information shall require a receipt only if the sender deems it necessary. 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, and retained for two years.

### Addressing Mail or Shipment of Classified Material

Mail or shipments containing classified material shall be addressed to the Commander or approved classified mailing address of a federal activity, or to a cleared contractor using the name and classified mailing address of the facility. An individual’s name shall not appear on the outer cover. This does not prevent the use of office code letters, numbers, or phrases in an attention line to aid in internal routing.

1. When necessary to direct SECRET or CUI material to the attention of a particular individual other than as prescribed below, the identity of the intended recipient shall be indicated on an attention line placed in the letter of transmittal or on the inner container or wrapper.

2. When addressing SECRET or CUI material to an individual operating as an independent consultant or to any facility at which only one employee is assigned, the outer container shall specify:

**‘‘TO BE OPENED BY ADDRESSEE ONLY’’   
*and be annotated:*    
  
 ‘‘POSTMASTER — DO NOT FORWARD.   
 IF UNDELIVERABLE TO ADDRESSEE, RETURN TO SENDER.’’**

### Use Of FedEx or Other Approved Couriers For Overnight Transmission Of Classified Information Within The Continental U.S.

The following requirements apply and *must be* explicitly followed:

1. FedEx or other approved courier may be used for the urgent overnight transmission of SECRET and CUI material within the continental United States when over­night delivery cannot reasonably be accomplished by the U.S. Postal Service. However, classified Communications Security (COMSEC), NATO, and foreign government infor­mation may ***not*** be transmitted via FedEx.
2. FedEx or other approved courier personnel should ***not*** be notified that the package contains classified material.
3. Material must be prepared for transmission as described in NISPOM paragraph 5-401a, except that a FedEx or other approved courier mailing envelope may be used as the outer wrapper.
4. The outer address label *(*Figure 4*)* block #3, shall be addressed to the *“Security Office”* or the “*Facility Security Officer”* of the destination facility.

***NISPOM Paragraph 5-401a. Preparation and Receipting***

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, and returned to the sender.

1. Senders may not use a post office (P.O.) box as the destination address because FedEx cannot deliver to a P.O. box. Instead, a street delivery address approved for overnight shipments by the recipient’s Cognizant Security Office (CSO) shall be obtained from the Central Verification Activity (CVA), **1-888-282-7682**. Identification of a contractor’s address in the CVA listing as an authorized overnight delivery address indicates CSO approval of the receiving facility’s ability to securely accept such packages.
2. To ensure direct delivery to the addressee, the release signature (block #8) on the FedEx or other approved courier airbill label may not be executed (Figure 4*).*
3. As a general rule, packages may be shipped on Monday through Thursday *only* to ensure that FedEx does not have possession of a package over a weekend.
4. **All employees who handle incoming FedEx or other approved courier shipments addressed to the Security Office or the Facility Security Officer must be cleared.**

***The use of external (street side) collection boxes is prohibited.***

|  |
| --- |
| Figure 4. Sample FedEx USA Airbill for Outgoing Packages |

### Receipt of FedEx or other Courier Addressed to “Security Office” or “FSO”

The following requirements apply and *must be* explicitly followed:

* When a FedEx package is addressed to either **‘‘Security Office’’** or **‘‘Facility Security Officer,’’** it **MUST** be signed for by either the **Facility Security Officer** or a **Designee** (Figure 5).

|  |
| --- |
| Figure 5. Sample FedEx USA Airbill for Incoming Packages |

In addition to FedEx, the General Services Administration (GSA) has currently approved eight other carriers as follows:

• Airborne Express

• AirNet Systems

• Associated Global Systems

• Cavalier Logistics Management

• CorTrans Logistics

• DHL Airways

• Menlo Worldwide Forwarding (formerly Emery)

• United Parcel Service.

**No matter which vendor is used follow the procedures outline for FedEx.**

### Transmission Outside the U.S., Puerto Rico, or U.S. Possession or Trust Territory

Classified material may be transmitted to a U.S. government activity outside the U.S., Puerto Rico, or a U.S. possession or trust territory only under the provisions of a classified contract or with the written authorization of the GCA.

SECRET and CUI may be transmitted by:

1. Registered mail through U.S. Army, Navy, or Air Force postal facilities;

2. An appropriately cleared contractor employee;

3. U.S. Civil Service employee or military person who has been designated by the GCA;

4. U.S. and Canadian registered mail with registered mail receipt to and from Canada and via a U.S. or a Canadian government activity; or

5. As authorized by the GCA.

***Gemini employees are not authorized to carry classified material across international boundaries.***

### Couriers, Hand-Carriers and Escorts

Appropriately cleared employees can be designated as couriers, hand-carriers, and escorts. An authorization letter on Gemini letterhead, which contains the employee’s name and Social Security number for identification will be prepared and signed by the FSO.

Appropriately cleared employees may hand-carry classified material aboard commercial passenger aircraft if authorized in writing by the Facility Security Officer or other cleared KMP.

Procedures contained in FAA Advisory Circular (AC) 108-3, ‘‘Screening of Persons Carrying U.S. Classified Material,’’ must be followed, and authorization will have to be provided to the traveler.

If the destination will take longer than a normal day’s travel time, arrangements will be made in advance of departure for overnight storage at a U.S. government installation or at a cleared con­tractor’s facility that has appropriate storage capability.

## HAND CARRYING OF CLASSIFIED DOCUMENTS AND HARDWARE

Classified documents shall not be hand-carried aboard commercial passenger aircraft unless authorized in writing by a Gemini cleared KMP. Travel authorization letters are available in the Security Office.

* Hand carrying of classified hardware or other bulky packages aboard commercial aircraft is prohibited unless specifically approved by DCSA.
* Gemini employees are not authorized to carry classified material across international boundaries.

A Gemini employee intending to hand-carry classified documents out of the facility is responsible for reading NISPOM Sections 5-409 through 5-413. Copies of these sections are available in the Security Office.

The person hand carrying the documents must sign a copy of the ‘‘In-Transit Receipt’’ to be left in the Security Office, the suspense file copy, and include two copies of the receipt in the double-wrapped package being carried. If the documents are not returned to Gemini, the recipient will sign a copy of the receipt and mail it back to Security, and retain the other copy.

If the document is returned by the courier, the receipt will be signed and dated by the courier and the document will be recorded in the proper manner.

If, during the hand carrying of any classified information, there is any threatened espionage, sabo­tage, subversive activities, loss, compromise, or suspected compromise of the classified infor­mation, the **NEAREST** office of the FBI is to be notified.

Additional requirements pertaining to the hand carrying of classified material other than docu­ments can be obtained in the Security Office.

Classified material handed into Gemini as the result of meetings, visits, etc., must be entered into Document Control accountability records. The material should be brought into the Security Office, where it will be assigned a document control number.

## HANDLING MATERIAL WITHIN A FACILITY

### TRANSMISSION OF MATERIAL WITHIN A FACILITY

SECRET and CUI material being transmitted within a facility must be in the pos­session of a responsible employee who is cleared to the level of the classified information and has a need-to-know authorization.

The material may be transmitted within a facility without double wrapping, but **MUST BE PROTECTED** from casual viewing and remain under the direct surveillance of the responsible employee at all times.

### Reproduction

Reproduction of classified material must not be done without the knowledge of the Security Officer. When it is necessary to make copies of classified material, two (2) cleared personnel always must be present.

1. The ‘‘Restricted Area’’ sign must be on the outside of the copy room door.

2. The copy room door must be closed and locked.

3. The copier/printer must be disconnected from the network.

4. Make copies as needed. Each copy made is assigned the same Document Control Accountability Number of the original material but marked ‘‘Copy 1 of X,’’ ‘‘Copy 2 of X,’’ ‘‘Copy 3 of X,’’ etc., and entered into the log.

5. Only make as many copies as needed to meet immediate requirements. (These copies are to be destroyed when no longer needed; *see Section 11.16 of this handbook for procedures regarding destruction of classified material.*)

*6.* After each copy job is completed, the Automatic Overwrite Program (DATACLEAR) starts and overwrites the image on the hard drive and RAM four (4) times. ***It is important to note that the user cannot stop this function.***

### Safeguards During Use

When not safeguarded by storage in authorized file containers and when in actual use by authorized personnel, classified material shall be protected as follows:

1. Kept under the constant surveillance of an appropriately cleared, authorized person, who is in a physical position to exercise direct security controls over the materials.

2. Covered by green transparent covers or in red binders or folders, turned face down, placed in storage containers, or otherwise protected, when unauthorized persons are present.

3. Returned to storage containers and secured as soon as practicable after use.

During classified reports preparation, working papers, notes, initial drafts, drawings, typewriter ribbons, carbon paper, etc., containing classified information shall be safeguarded according to the highest classification of the information contained therein.

All storage containing classified material shall be secured at all times when not under the direct supervision of a cleared person with authority for access to the information therein.

A written log, displayed on the container, will be signed by an authorized individual (Facility Security Officer or other designated individual) at the end of each day verifying that the safe is locked and secured.

The Security Officer may, at his/her discretion, invoke a rotational security check in which all cleared individuals take a weekly turn at the daily inspection.

Perimeter control checks will be conducted simultaneously with self-inspections. All persons who enter or exit the facility shall be subjected to a *random* inspection when the possibility of access to classified material is remote. Inspections are not required of wallets, change purses, clothing, cosmetic cases, or other objects of an unusually personal nature. A written notice of the policy will be visibly displayed.

### Destruction

Classified waste shall be destroyed as soon as practical.

During self-inspections, the classified material list should be reviewed by Contract Managers to reduce classified material to the minimum necessary for effective and efficient operations.

Gemini is required to destroy classified material in its possession, unless otherwise notified in writing by the Contracting Officer, as soon as practicable after it has served its purpose. This includes material released by the government; developed or prepared by Gemini; or retained after completion or termination of the contract.

Classified material may be retained for a period of 2 years after completion of the contract if the material was received or generated under a contract. If retention is required beyond the 2-year period, the contractor must request and receive written retention authority from the Government Contracting Activity (GCA).

Classified material to be destroyed should be brought to the Security Office, where accountability records will be adjusted and material will be recorded on a Preparation for Document Destruction Log (Figure 6).

|  |
| --- |
| Figure 6. Preparation for Document Destruction Log |

Typewriter and automatic data processing equipment ribbons used in transcribing classified material shall be safeguarded according to the classification of the material on which they are used. Typewriter film ribbons, which are used only once and contain classified information, must not be left in the typewriter unprotected at any time (i.e., during coffee breaks, lunch hours, errands, etc.) and are to be destroyed as soon as possible as classified waste.

Destruction will be accomplished by shredding the classified material with the use of the approved SEM 224 shredder. ***A cleared Gemini employee who has knowledge of the material, as well as a cleared witness, will be present at the time of destruction.***

After destruction of the classified material has been accomplished, ***both employees will be required to sign the Destruction Certificate*** (Figure 7). The signed certificate is to be given to the FSO and keep on file in the Security Office. Destruction records and certificates are maintained by the FSO for a minimum of two years.

|  |
| --- |
| Figure 7. Destruction Certificate |

# MARKING CLASSIFIED MATERIAL

## GENERAL

Classification designation by physical marking, notation, or other means serves to warn and inform the holder as to what degree of protection against unauthorized disclosure is required for that information or material. Other notations facilitate downgrading and declassification, and aid in derivative classification actions. Therefore, it is essential that all classified information and material be marked in such a manner that it is clear to the information or material; exactly what portions of the information or material contain or reveal classified information; how long the protection is required; and any other additional markings that are required for the protection of the information or material.

The DoD requiring activity is responsible for identifying covered defense information (CDI) in accordance with DoD procedures for identification and protection of controlled unclassified information found in DoDM 5200.01 Vol 4, DoD *Information Security Program*: *Controlled Unclassified Information (CUI).* The requiring activity is also responsible for determining the appropriate marking for the CDI in accordance with the procedures for applying distribution statements on technical documents found in DoDM 5200.01 Vol 4 and DoDI 5230.24, *Distribution Statements on Technical Documents*. The requiring activity must document in the Statement of Work that CDI is required for performance of the contract, and specify requirements for the contractor to mark the CDI developed in the performance of the contract.

Refer to *DoD Guide to Marking Classified Documents* (DoD 5200.1-PH) for samples of documentation markings.

## CLASSIFICATION ROLES AND RESPONSIBILITIES

### Security Classification Guidance

Appropriate security classification guidance information is provided to the contractor on the Security Classification Specification. DD Form 254 is the only document authorized for use in conveying security classification guidance, and regarding, downgrading, and declassification instructions to a contractor. It is the contractor’s responsibility to understand and apply all aspects of the classification guidance.

Contractors may submit recommended changes for a revised DD Form 254 if they encounter difficulty applying or interpreting the DD Form 254 during any phase of the contract. Clas­sification guidance is, notwithstanding the contractor’s input, the exclusive responsibility of the User Agency, and the final determination of the appropriate classification for the information rests with that Agency. The CSO may be requested to provide assistance, if desired.

### Roles and responsibilities

The Project Manager directs the appropriate classification markings on classified material generated in con­nection with the classified contract.

Any person (employee) reproducing, copying, or otherwise creating classified material is responsible to ensure that the material is appropriately marked. The Security Officer should be contacted if there are any questions as to the appropriate markings. The Contract Security Classification Speci­fication or Classification Guides should be referred to when creating classified documents.

Contractors who subcontract with another contractor assume responsibilities similar to those of a User Agency.

## MARKINGS

### 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.

### Initial Markings

This applies to paper copies of documents overall and page markings. The overall classification of a document, whether it be a letter, report, message, pamphlet, etc., shall be immediately and conspicuously marked at the top and bottom on the outside front cover or ‘‘face’’, title page, first page, and outside back cover.

The front cover or ‘‘face’’ of a document must show, in addition to the overall classification at the top and bottom, one of the additional marking notations; that is, either the downgrading and declassification notice or one of the Restricted Data notations, the date of preparation and the name and address of the facility preparing the document, and the UTRS document control number.

In the absence of a front cover, this information must be shown on the title page or the first page.

### Portion Markings

Each section, part, paragraph, or similar portion of a classified document shall be marked to show the highest level of its classification or that the portion is unclassified. In marking portions, the parenthetical symbols (TS) for TOP SECRET, (S) for SECRET, (CUI) for CONFIDENTIAL, and (U) UNCLASSIFIED shall be used.

The basic rules for portion markings are:

1. Mark each portion clearly to eliminate doubt as to the level of classification.
2. All classified and unclassified information must be identified within a document.
3. Mark each portion with its highest classification.
4. Mark each portion immediately following its number or letter designation, or before it begins, if there is no number or letter designation.

In addition, portions that contain CNWDI information will be marked (N) following the classifica­tion, i.e., (TS-RD) (N).

All classified documents created by Gemini shall be portion marked, unless otherwise directed. Any portion extracted from a NATO document that is not portion marked, must be assigned the classification that is assigned to the NATO document.

a. All U.S. originated NATO classified documents shall bear an assigned reference number and date on the first page. The reference numbers shall be assigned as follows:

(1) The first element shall be the abbreviation for the name of Gemini Tech­nologies, Inc., which is Gemini.

(2) The second element shall be the abbreviation for the overall classification followed by a hyphen and the four-digit sequence number for the document within that classification that has been generated for the applicable calendar year.

(3) The third element is the year; e.g., Gemini/NS-0013/93.

b. COSMIC TOP SECRET, NATO SECRET, and ATOMAL documents shall bear the reference number on each page and a copy number on the cover or first page. Copies of NATO documents shall be serially numbered. Pages shall be numbered. The first page or index or table of contents shall include a list, including page numbers, of all Annexes and Appendices. The total number of pages shall be stated on the first page. All Annexes or Appendices will include the date of the original document and the purpose of the new text (addition or substitution) on the first page.

c. One of the following markings shall be applied to NATO documents that contain ATOMAL information:

(1) ‘‘This document contains U.S. ATOMIC Information (RESTRICTED DATA or FORMERLY RESTRICTED DATA) made available pursuant to the NATO Agreement for Cooperation Regarding ATOMIC Information, dated 18 June 1964, and will be safeguarded accordingly.’’

(2) ‘‘This document contains UK ATOMIC Information. This information is released to the North Atlantic Treaty Organization including its military and civilian agencies and member states on condition that it will not be released by the recipient organization to any other organization or government or national of another country or member of any other organization without prior permission from H.M. Government in the United Kingdom.’’

d. Working papers shall be retained only until a final product is produced.

### Additional Markings

The appropriate notation shall be printed, stamped, typed, or otherwise affixed conspicuously at least once on all classified material possessed, prepared, or reproduced at Gemini. In addition, when a copy, extract, or paraphrase of a document contains classified information, it shall also be marked conspicuously at least once with the appropriate notation. In the case of documents, these warning notices shall be conspicuously marked on the outside of the front cover (if any) or on the first page if there is no front cover. When display of warning notices on other materials is not feasible, the warnings shall be included in the written notification of the assigned classification.

### Derivative classification

### Dates or events carried forward

Downgrading or declassification dates or events required on the markings shall be carried forward and applied whenever the classified information is incorporated in new material generated at a later time.

### Changing classification markings

When classification markings are changed or canceled, an entry shall be made in the document accountability records to reflect such a change or cancellation.

### Release of declassified information

Declassification of information either automatically or by individual review and determination is not automatically an approval for public release. Accordingly, the contract administrator will request permission to release

### Downgrading/declassification and “Classified by” line procedures

All derivatively classified material shall be marked to reflect declassification instructions, the source of classification and, if applicable, downgrading instructions. Documents shall show the required information either on the cover, title page, first page, and outside on the back cover. Other material shall show the required information on the material itself, or if not practical, in related or accompanying documentation.

The markings used to show this information shall be as follows:

CLASSIFIED BY (Required)

DOWNGRADE TO on (As Appropriate)

DECLASSIFY ON (Required)

In completing the ‘‘Classified By’’ line, Gemini shall identify the applicable DD Form 254 or other User Agency guidance. In addition, if any single guidance source other than or supplemental to the applicable DD Form 254 is followed, that source will also be shown in such a way that, standing alone, it will be sufficiently complete to identify it, including its date. If two or more guidance sources other than or in addition to the applicable DD Form 254 are followed by the phrase “Multiple Sources” Gemini will maintain adequate records to support application of the classification marking and retain such records for the duration of the contract or program under which the document was created. The records could take the form of a bibliography identifying the applicable classification sources and be keyed to the text.

Identification of the applicable DD Form 254 in the ‘‘Classified by’’ line will always include at least the date of the DD Form 254, and the specific contract number or other requirements document for which the DD Form 254 was issued.

In completing the ‘‘Declassify on’’ line, Gemini shall use the information specified in or with the DD Form 254 provided by a User Agency or shown on a source document.

In completing the ‘‘Downgrade to’’ line, Gemini shall insert SECRET or CUI, and an effective date or event as indicated in or with the DD Form 254, or as shown on a source document.

# SAFEGUARDING CLASSIFIED INFORMATION

## CONTROL OF AREAS

***This section does not currently apply to Gemini. Gemini is not a “retaining” facility and therefore does not have approval for retention of classified material. These sections have been included as a reference and training guide for future implementation when the time arises*.**

### GENERAL

If the classified material is of a nature and size that prevention of unauthorized access and assurance of adequate protection from compromise has not been accomplished by use of approved containers, this method qualifies as authorized storage for classified materials when not in use.

Classified information and CUI shall be protected at all times. When this cannot be adequately accomplished, it is necessary to employ additional safe­guarding methods and designate the area as controlled.

There are two types of controlled areas: closed and restricted.

### Closed Area

A closed area is one in which classified material, because of its nature or size, cannot be adequately stored in approved containers during non-working hours and visual access cannot be prevented by usual methods while work is in progress. The control requirements for this type of area may be found in paragraph 5-306 of the NISPOM.

### Restricted Area

A restricted area is one in which classified material can be stored in approved containers during non-working hours, but visual access cannot be prevented by the usual methods while work is in progress. The necessary controls are as follows:

1. Area will be posted with sign(s) stating:

‘‘Restricted Area  
Classified Work in Progress  
Authorized Personnel Only’’

2. During Working Hours— Area will be controlled by appropriately cleared personnel who will prevent unauthorized persons from gaining access.

3. During Non-working Hours — Classified material shall be stored in approved containers as described in the ‘‘Storage’’ section of this SPP.

Perimeter control checks will be conducted simultaneously with self-inspections. All persons who enter or exit the facility shall be subject to a random inspection where the possibility of access to classified material is remote. Inspections are not required of wallets, change purses, clothing, cosmetic cases, or other objects of an unusually personal nature. A written notice of this policy will be visibly displayed.

## STORAGE OF CLASSIFIED MATERIAL

***This section does not currently apply to Gemini. Gemini is not a “retaining” facility and therefore does not have approval for retention or storage of classified material. These sections have been included as a reference and training guide for future implementation when the time arises*.**

### SECRET Material

SECRET material, when not in use, must be stored in a GSA-approved safe with a three-position combination lock. The security container would be located in the Facility Security Officer’s office.

* The combinations will be changed at least once a year and at the earliest practicable time after: the reassignment, transfer, or discharge of any person having knowledge of the combination; the security clearance has been downgraded to a lower level than the material stored; or compromise is suspected.
* A minimum of authorized persons shall possess the combinations to the storage container(s) or have access to the information stored therein. Names of individuals with safe access should be clearly displayed on the safe.
* The Security Office will keep a record of the names of all those having knowledge of each com­bination. In the event it is necessary for an employee to gain access to material in a file, the Security Officer will ascertain the need-to-know, open the safe, locate the document, and forward it to the requester.

**COMBINATIONS WILL BE MEMORIZED AND NOT WRITTEN DOWN.**

Report any damage to GSA-approved file cabinets holding classified material to the Security Officer immediately. **DO NOT** attempt to repair or restore the integrity of any GSA approved file cabinet.

Repairs to the cabinet will be arranged for by the FSO with the following:

SM Services

Division of Safemasters

458 North 2nd Street

Philadelphia, PA 19123

Phone: (215) 413-3920

Fax: (215) 413-2712

[www.safemasters.com](http://www.safemasters.com)

or other approved repair companies.

Insofar as possible, all classified material will be consolidated and regularly evaluated in order to minimize the number of classified cabinets required.

If the container is used for special categories of information, such as NATO, Critical Nuclear Weapons Design Information (CNWDI), Restricted Data, or other information that requires special briefings or access requirements, access to the combination record shall be controlled and restricted to persons who have a need to know.

### CUI Material

Covered defense information is used to describe information that requires protection under DFARS Clause 252.204-7012. It is defined as unclassified controlled technical information (CTI) or other information as described in the CUI Registry (http://www.archives.gov/cui/registry/category-list.html), that requires safeguarding/dissemination controls AND IS EITHER marked or otherwise identified in the contract and provided to the contractor by DoD in support of performance of the contract; OR collected/developed/received/transmitted/used/stored by the contractor in performance of contract.

Operationally critical support is defined as supplies/services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

To safeguard covered defense information contractors/subcontractors must implement NIST SP800-171, Protecting CUI in Nonfederal Information Systems and Organizations.

Controlled Unclassified Information is similar to FOUO as it is handled, stored, transmitted, and destroyed in basically the same manner as the legacy FOUO program:

* When the option is available, should be processed on Government Furnished Equipment (GFE).
* Must be encrypted if sent via NIPRNet.
* Limit access to those with a lawful government purpose.
* Destroyed by means approved for destroying classified or in a manner making it unreadable, indecipherable, and irrecoverable.

CUI material, when not in use, will be stored in the same manner as SECRET. After working hours, CUI will be stored in unlocked containers, desks, or cabinets if the government building provides security for continuous monitoring of access. If building security is not provided, the information will be stored in locked desks, file cabinets, bookcases, locked rooms, or similarly secured areas.

## Digital Documentation Handling

The increasing digital nature of information, documents, and system accesses has spawned a heightened need for strong processes and measures to enhance cybersecurity. Online threats from adversaries are more prevalent, and attacks can present themselves through e-mail, website hacks, phishing, and more.

### Transmission of Documentation

Documentation considered sensitive or classified must be transmitted via a government-approved secure method. Contractors can only handle SECRET documentation if they are NIST CMMC certified, and implement the processed approved by that method. *Gemini is currently preparing for potential CMMC certification*.

Government representatives can utilize the DoD SAFE digital file sharing tool to send CUI documents via the web over a safe, encrypted link to specific recipients. Additionally, government POCs and contractors can create a secure handshake using encrypted e-mails, or CUI documentation can be packaged in a secure, encrypted pdf.

1. Employee created a secure envelope pdf that is password protected.
2. Employee sends password via separate e-mail to intended recipient.
3. Secure envelope is attached to e-mail with a non-specific subject line.

### Access Controls and Cybersecurity

To report cyber incidents that affect covered defense information or that affect the contractor’s ability to perform requirements designated as operationally critical support, the Contractor shall conduct a review for evidence of compromise and rapidly report cyber incidents to DoD athttps://dibnet.dod.mil via an incident collection form (ICF).

* If discovered and isolated in connection with a reported cyber incident, the contractor/subcontractor shall submit the malicious software to the DoD Cyber Crime Center (DC3).
* If DoD elects to conduct a damage assessment, the Contracting Officer will be notified by the requiring activity to request media and damage assessment information from the contractor.

# SECURITY VIOLATIONS AND INFRACTIONS

## GENERAL

Immediately following a security violation, the FSO will notify the appropriate Division Manager in writing, setting forth all available information concerning the violation and requesting the determination of certain essential elements of information. This notification will always include a suspense date for replying.

Upon determining the individual responsible for the violation, the FSO may direct that all government classified information be removed from the individual’s custody and that all access be denied pending further investigation.

In all cases in which government classified information is removed and access denied an individual, a review will be made by the Division Director and the FSO to determine the final action to be taken. In cases of disagreement, the concerned Division Manager and the Human Resource Manager will determine the final action to be taken.

If, in any security violation, it is determined or suspected that government classified information or material has been released to, or taken by, unauthorized individuals, the FSO is required to report the incident within 48 hours to the FBI at (215) 418-4000.

## ADMINISTRATIVE MEASURES

Gemini has established policies that provide for appropriate administrative actions against employees who violate the requirements of the NISPOM. Based on the severity of the violation, disposition of alleged offenses, as a result of investigation, may be subject to: counseling, written letter of caution, final written warning, disciplinary suspension, or dismissal.

In all cases where a breach of security occurs, whether major or minor, a brief summary of the event will be filed in the employee’s personnel record. The following administrative measures will be taken in the order listed below when a security violation occurs.

1. **First Violation**: — The employee will receive a written letter of caution.
2. **Second Violation**: — The employee will receive a Final Written Warning which could include a disciplinary suspension without pay for not less than one working day, and not more than 15 working days or dismissal.

# REPORTING REQUIREMENTS

As a cleared contractor, Gemini has a responsibility to report certain events that have an impact on the status the company’s FCL, or an employee’s PCL, that affect proper safeguarding of classified information, or that indicate classified information has been lost or compromised. Gemini will provide complete information to enable the CSA to ascertain whether classified information is adequately protected. Gemini will submit the reports as follows.

1. When reports are classified or offered in confidence and so marked by Gemini, the information will be reviewed by the CSA to determine whether it may be withheld from public disclosure under applicable exemptions of the Freedom of Information Act   
   (5 U.S.C. 552).
2. When reports are unclassified and contain information pertaining to an individual, the Privacy Act of 1974 (5 U.S.C. 522a) permits withholding of that information from the individual only to the extent that the disclosure of the information would reveal the identity of the source that furnished the information.

## REPORTS TO THE COGNIZANT SECURITY AGENCY (CSA)

Gemini will submit the following reports to the CSA, as appropriate.

1. Any adverse information that indicates that an employee’s access to classified infor­mation may not be clearly consistent with the national interest. *Reports based on rumor or innuendo should not be made.*

As a general rule, any information that reflects adversely on the integrity or character of an employee, which suggests that his or her ability to safeguard classified information may be impaired, should be reported to the CSA.

Refer to NISPOM paragraph 1-302 for the acceptable format when submitting a report. *Subsequent discharge of an individual by Gemini does not make it unnecessary to submit a report.*

2. Suspicious contacts, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee. Also includes all contacts by cleared employees with known or suspected intelligence officers from any country.

3. Change in employee’s status:

a. Death

b. Change in name

c. Termination of employment

d. Change in marital status *(Top Secret only)*

e. Change in citizenship.

f. When the possibility of access to classified information in the future has been reasonably foreclosed.

4. 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

5. Citizenship by naturalization. A non-U.S. citizen granted a Limited Access Authoriza­tion (LAA) who becomes a citizen through naturalization.

6. Employees desiring not to perform on classified work. Evidence that an employee no longer wishes to be processed for a clearance or to continue an existing clearance.

7. Refusal of an employee to execute the Classified Information Nondisclosure Agreement (SF 312).

8. Changes affecting the Facility clearance.

a. Any change of ownership including stock transfers.

b. Any change of company operating name or address or any of its cleared locations.

c. Any change to the information previously submitted for key management personnel (KMP).

9. Action to terminate business or operations, including bankruptcy.

10. Any material changes concerning the information previously reported concerning Foreign Ownership, Control, or Influence (FOCI).

11. Change in storage capability.

12. Inability to safeguard classified material.

13. Security Equipment vulnerabilities.

14. Unauthorized receipt of classified material.

15. Employee Information in compromise cases.

16. Disposition of classified material terminated from accountability.

17. Foreign Classified contracts.

## REPORTS TO THE FBI

Gemini is required to submit a report in writing to the nearest office of the FBI, classified, if appropriate, concerning actual, probable or possible espionage, sabotage, or subversive activities at any of Gemini’s locations. An initial report may be made by phone, but must be followed in writing. A copy of the written report will be provided to the CSA.

If the time is of the essence and the report is made by phone, it must be followed in writing and addressed as follows:

Federal Bureau of Investigation (FBI)

William J. Green, Jr. Building

600 Arch Street, 8th Floor

Philadelphia, PA 19106

Phone: (215) 418-4000

# OPERATIONS SECURITY (OPSEC)

This section of the manual provides information and guidance for uniform implementation of the DoD OPSEC program when contractually imposed on Gemini.

OPSEC is a DoD directed effort. Its principal objective is to preclude the disclosure of classified information by denying or reducing the opportunity of Hostile Intelligence Services (HOIS) to gain access by directly observing/analyzing/evaluating our activities and operations, the awareness of which may lead to the compromise of classified information. Stated another way, OPSEC is the method of identifying, controlling, and protecting critical information; analyzing friendly actions and indicators that would allow adversaries or potential adversaries to identify and exploit vulnerabilities; and a cyclic assessment of effectiveness to deny information to an adversary (Figure 8).

|  |
| --- |
| Figure 8. OPSEC Cycle |

The general aim of OPSEC is to promote mission effectiveness by preserving essential secrecy about U.S. intentions, capabilities, and current activities when the procedures for safe-guarding classified material and information require enhancement. Secrecy essential to defense activities may be compromised whenever open sources (such as technical articles, press releases, National Technical Information Service publications, the Congressional Record, Commerce Business Daily, or contract awards) and detectable activities (such as communications, logistics actions, research, development and test activities, or radar emissions) provide information that hostile intelligence can piece together or analyze, resulting in adversary actions harmful to U.S. interests. In some instances, such information or indicators/activities are unprotected or not addressed by the DISP requirements for classified material and require case-by-case planning to identify them. The fundamental goal of the OPSEC process is to minimize or eliminate such indicators. OPSEC thus encompasses activities, which are unique to the OPSEC process, i.e., a) determining, through threat/vulnerability analysis, whether there are unacceptable/undesirable intelligence indicators and what they are; b) developing and implementing countermeasures to best eliminate or minimize them.

OPSEC is concerned with all sources of exploitable information. OPSEC is principally oriented to those instances in which evaluations indicate program weakness, which could lead to the disclosure of classified information.

OPSEC will be directed to the protection of unclassified intelligence indicators on classified programs of such a nature that the disclosure of the indicators may lead to the compromise of classified information. OPSEC is not intended as a vehicle to protect unclassified technology.

Specific detailed UA requirements for OPSEC shall be included in appropriate requisition docu­mentation and resultant contract or addendum thereto in sufficient detail to ensure complete contractor understanding of exactly what special OPSEC provisions or measures are required by the UA. In providing such measures, UAs shall not solely refer to their internal regulations in the contract proper and shall provide necessary information to fully explain internal regulations. Additionally, applicable DD 254s will be annotated to indicate that OPSEC requirements are contained in the contract or addendum thereto.

Full and detailed OPSEC contract and subcontract requirements to include Contract Security Classification Specification will be provided to DCSA CSOs by UAs pass or prime contractors as appropriate. When required, employees access OPSEC training via the DoD education website: <https://securityawareness.usalearning.gov/opsec/index.htm> .

DCSA has principal responsibility for inspecting Gemini compliance with OPSEC requirements. Cognizant UA representatives may accompany DCSA if requested. OPSEC inspections will be accomplished:

1. As part of a regularly scheduled industrial security inspection.
2. As part of an unannounced industrial security inspection.

## INSIDER THREATS

A growing area of security concern is with insider threats. Insider threats can be intentional espionage by embedded enemy actors, a willful act of classified information sharing on the part of a cleared employee with no obvious foreign connections, or an “accidental” sharing of classified information with a bad actor by an unwitting cleared employee.

### General

Executive Order 13587 establishes the requirement for government agencies to establish their own insider threat programs. This Order defines the insider threat program purpose as deterring, detecting, and mitigating insider threats. Insider threat programs are intended to: Deter cleared employees from becoming insider threats; detect insiders who pose a risk to classified information; and mitigate the risks through administrative, investigative, and other response actions.

### Targeted Individuals

Of special focus for adversaries is the research and academic fields. Specific planned programs targeting these areas are intended to steal information and weaken the U.S industrial base. Any employees who work with research or academic professionals on projects that may have significance for any industrial or military use should have heightened awareness of the risk and we watchful of potential infractions of security policy.

### Threat Intelligence

The FSO is responsible for being aware and abreast of current threat intelligence. This is enabled by

1. Reviewing and disseminating pertinent intel from DCSA regular unclassified briefings.
2. Monitoring media and news outlets on a regular basis to identify security violation “stories” that can be used for employee education.

### Employee Training

Employee education about identifying insider threats is a critical issue for all contractors working on defense and Federal work. Continual education about the evolving face of insider threats is a task implemented by the FSO. Regular review of the monthly DCSA cleared briefing and subscribing to the periodic BTAC Insider Threat newsletters provides validated information sources to support regular and current employee briefings and communications. Insider threat information is included in:

1. New employee onboarding training, for both cleared and uncleared employees.
2. Annual Security Refresher training.
3. Periodic briefings, typically spawned by a specific threat identified via:
   1. Counterintelligence briefings from BTAC or DCSA.
   2. Infraction published in the media.

### Reporting Insider Threats

If any employee sees, hears, or suspects a risk or threat internal to a project, program or the company, they should report this to their FSO for investigation. Employees are apprised of the DoD Hotline for reporting threats.

## ANALYSIS OF EXTERNAL THREATS

Intelligence Collection, the world of espionage and counterespionage, spies and spy catchers, is a popular subject of fiction. It has been the topic of countless books, short stories, TV serials, and movies. The role of the spy, the ‘‘Secret Agent,’’ has become so sensationalized and exaggerated that it is very easy to think that spies exist only in the minds of fiction writers, that spying belongs in the same category as science fiction and westerns. Do not believe it. Spies do exist, and literally thousands of spies, or intelligence officers, as they are officially known, and terrorists, are at this moment plying their treacherous trade within the U.S.

### Counterintelligence Awareness

Counterintelligence awareness is critical. There has been a long standing, well-organized, deliberate, and quite successful effort to acquire and utilize Western state-of-the-art technology by both overt and covert means. Unquestionably, this acquisition of Western technology has played, and will continue to play, an extremely important role in the development of industrial and military capabilities of hostile countries. A philosopher once said, ‘‘Knowledge itself is power.’’ This maxim most certainly applies to national power, for one gauge of national power is the amount and quality of scientific, technological, and military-related knowledge possessed by a nation.

A nation such as the U.S. can be weakened by the theft of its vital knowledge, and its enemies can be strengthened by the acquisition of that knowledge, whether it be classified or unclassified. It is the responsibility of each individual who has been entrusted with sensitive data to do his or her share in protecting America’s strategic knowledge, whether it is classified TOP SECRET or seemingly unimportant, unclassified material. If Americans do not conduct themselves in a responsible and patriotic manner, and do not recognize that this country’s national security is based essentially on the loyalty and efforts of its citizens, then the tightest document classification system, the most efficient security organization, and the mightiest armed forces may be utterly valueless.

### Counterintelligence Objectives

The main objective of spies is the wholesale collection of data. The most prized type of intel­ligence data is the classified Government document, but unclassified material, even material that appears to be trivial, can also be of inestimable value. In their task of gathering intelligence data, the foreign intelligence services have a large array of tools. Satellites miles above the Earth’s surface gather photographic data. Aircraft and vessels gather electronic intelligence. But a further source of data, and potentially the most valuable to a hostile group, is that acquired through the use of actual spies. Intelligence services may gather their information through the use of several different techniques. Probably the greatest achievement any intelligence organization can have is the placement or recruitment of an agent directly in a sensitive position in a national defense or intelligence element of an opposing Government. Elicitation by foreign intelligence officers or terrorists is a commonly used and effective way of subtly collecting information through what appears to be normal, perhaps even mundane, social or professional conversation. The penetration by live or electronic sources of private institutions involved in sensitive, national defense-related research and development work can also be of tremendous value

### Protecting the Parts

It cannot be overemphasized that unclassified material may be unjust as valuable to a foreign intelligence service as classified material. In formulating their estimations of U.S. strengths and weaknesses and in the quest for data that will enhance their own nation’s strength, foreign intelligence services seek all types of material. A small bit of information could represent a very important piece in a much larger puzzle. Therefore, all data should be protected from the probing hands of foreign agents. A stolen industrial process can save thousands of dollars in research and development cost. The most trivial document could be the missing link of a hostile nation’s problem.

### Reporting the Threat

Each U.S. Government Agency and private industry which deals with classified material has a specified official in charge of security matters. The Facility Security Officer should be recognized as an ally and not an adversary. If approached by a suspicious stranger in the manner described above, the FSO should be informed immediately of the encounter. Even if a friendship has been established, even if the individual has been able to pry loose some information, the FSO should be consulted.

A major aspect of the FSO’s job is to protect employees from getting involved in compromising situations and, if necessary, to extricate them from such situations. Such assistance cannot be rendered if the employee remains silent. Of course, it is much better for an employee to reveal a suspect relationship voluntarily, rather than have it come to light in the course of a security investigation, or through some other means. Then, it may be too late for anyone to assist the indiscreet employee. Basically, it cannot be overemphasized that, if involved in a compromising situation the sooner the employee consults his or her FSO, the better.

Of course, sometimes one will be in a place or situation where one cannot, or for some reason does not want to, contact the FSO. Remember that in the U.S. the FBI is as close as the nearest telephone. Directions for contacting FBI offices appear in the front of all U.S. telephone books. Abroad, the nearest U.S. diplomatic establishment can arrange to put one in touch with the FBI or other appropriate U.S. Government security officials. It must be stressed that the best course of action in any questionable situations is to immediately contact a counterintelligence professional, who will analyze the situation and propose a course of action. Counterintelligence is a demanding and professional discipline, and any attempts by untrained amateurs to handle hostile efforts on their own could not only result in personal disaster, but also interfere with the FBI’s coordinated counterattack.

# Appendix A - Definitions

**Access.** The ability and opportunity to obtain knowledge of classified information.

**Adverse Information**. Any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security.

**Affiliate**. Any entity effectively owned or controlled by another entity.

**Approved Access Control Device.** An access control device that meets the requirements of the NISPOM as approved by the FSO.

**Approved Built-in Combination Lock.** A combination lock, equipped with a top-reading dial, that conforms to Underwriters’ Laboratories, Inc. Standard Number, UL 768, Group 1R.

**Approved Combination Padlock**. A three-position dial-type changeable combination padlock listed on the GSA Qualified Products List as meeting the requirements of Federal Specification FF-P-110.

**Approved Electronic, Mechanical, or Electro-Mechanical Device**. An electronic, mechanical, or electro-mechanical device that meets the requirements of the NISPOM as approved by the FSO.

**Approved Key-Operated Padlock**. A padlock, which meets the requirements of MIL-SPEC-P-43607 (shrouded shackle), National Stock Number 5340-00-799-8248, or MIL-SPEC-P-43951 (regular shackle), National Stock Number 5340-00-799-8016.

**Approved Security Container**. A security file container, originally procured from a Federal Supply Schedule supplier that conforms to federal specifications and bears a ‘‘Test Certification label’’ on the locking drawer attesting to the security capabilities of the container and lock. Such containers will be labeled ‘‘General Services Administration Approved Security Container’’ on the face of the top drawer. Acceptable tests of these containers can be performed only by a testing facility specifically approved by GSA.

**Approved Vault**. A vault that has been con­structed in accordance with the NISPOM and approved by the CSA.

**Approved Vault Door**. A vault door and frame unit originally procured from the Federal Supply Schedule (FSC Group 71, Part III, Section E, FSC Class 7110), that meets Federal Specification AA-D-600.

**Authorized Person**. A person who has a need-to-know for classified information in the performance of official duties and who has been granted a personal clearance at the required level.

**Automated Information System**. An assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information, and textual material.

**Automated Information System Security**. All security safeguards needed to provide an acceptable level of protection for Automated Information Systems and the classified data processed.

**Classified Authority**. The authority that is vested in a government official to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

**Classified Contract**. Any contract that requires or will require access to classified information by a contractor or his or her employees in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified.) The requirements prescribed for a ‘‘Classified contract’’ also are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other Government Contracting Agency program or project which requires access to classified information by a contractor.

**Classification Guide**. A document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specific information to be classified on a derivative basis. (Classification guides are provided to contractors by the Contract Security Classification Specification.)

**Classified Information**. The term includes National Security Information, Restricted Data, and Formerly Restricted Data.

**Classified Information Procedures Act**. A law that provides a mechanism for the courts to determine what classified information the defense counsel may access.

**Classified Visit**. A visit during which the visitor will require, or is expected to require, access to classified information.

**Classifier.** Any person who makes a classifica­tion determination and applies a classification category to information or material. The determi­nation may be an original classification action or it may be a derivative classification action. Con­tractors make derivative classification action. Contractors make derivative classification determi­nations based on classified source material, a security classification guide, or a Contract Security Classification Specification.

**Cleared Commercial Carrier**. A carrier that is authorized by law, regulatory body, or regulation to transport SECRET material and has been granted a SECRET facility clearance.

**Cleared Employees**. All contractor employees granted a personnel security clearance (PCL) and all employees in process for a PCL.

**Closed Area**. An area that meets the require­ments of the NISPOM, as approved by the CSA, for the purpose of safeguarding classified material that, because of its size or nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during non-working hours in approved containers.

**Cognizant Security Agency**. Agencies of the Executive Branch that have been authorized by E.O. 12829 to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released to U.S. Industry. These agencies are: The Department of Defense, the Department of Energy, the Central Intelligence Agency, and the Nuclear Regulatory Commission.

The Secretary of Defense (SECDEF) has been designated as Executive Agent for the NISP. Heads of the Executive Branches are required to enter into agreements with the SECDEF that establish the terms of the SECDEF’s responsibilities on behalf of these agency heads for administration of industrial security on their behalf.

**Cognizant Security Office.** The office or offices delegated by the Head of a CSA to administer industrial security in a contractor’s facility on behalf of the CSA.

**Colleges and Universities.** All educational institutions that award academic degrees, and related research activities directly associated with a college or university through organization or by the articles of incorporation.

**Communications Intelligence**. Technical and intelligence information derived from foreign communications by other than the intended recipient.

**Communications Security**. Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to national security and to ensure the authenticity of such communications.

**Company**. A generic and comprehensive term which may include sole proprietorships, individuals, partnerships, corporations, societies, associations, and organizations usually established and operating to com­monly prosecute a commercial, industrial or other legitimate business, enterprise, or undertaking.

**Compromise**. The disclosure of classified information to an unauthorized person.

**CONFIDENTIAL**. The designation that shall be applied to information or material the unauthor­ized disclosure of which could be reasonably expected to cause damage to the national security.

**Consignee.** A person, firm, or government activity named as the receiver of a shipment; one to whom a shipment is consigned.

**Consignor.** A person, firm, or government activity by whom articles are shipped. The consignor is usually the shipper.

**Constant Surveillance Service**. A transporta­tion protective service provided by a commercial carrier qualified by MTMC to transport CONFIDENTIAL shipments. The service requires constant surveillance of the shipment at all times by a qualified carrier representative, however, a facility clearance is not required for the carrier. The carrier providing the service must maintain a signature and tally record for the shipment.

**Continental Limits of the United States**. U.S. territory, including the adjacent territorial waters located within the North American continent between Canada and Mexico.

**Contracting Officer**. A government official who, in accordance with departmental or agency procedures, currently is designated as a contracting officer with the authority to enter into and administer contracts, and make determinations and findings with respect thereto, or any part of such authority. The term also includes the designated representative of the contracting officer acting within the limits of his or her authority.

**Contractor.** Any industrial, educational, commercial, or other entity that has been granted an FCL by a CSA.

**Courier**. A cleared employee, designated by the contractor, whose principal duty is to transmit classified material to its destination. The classified material remains in the personal possession of the courier except for authorized overnight storage.

**Conversion Rights**. The right inherent in the ownership or holding of particular securities to exchange such securities for voting securities.

**Critical Nuclear Weapon Design Information**. A DoD category of weapon data designating TOP SECRET Restricted Data or SECRET Restricted Data revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munition, or test device.

**Custodian**. An individual who has possession of, or is otherwise changed with, the responsibility for safeguarding classified information.

**Declassification**. The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, together with removal or cancellation of the classification designation.

**Declassification Event**. An event that eliminates the need for continued classification of information.

**Defense Transportation System**. Military controlled terminal facilities, Military Airlift Command controlled aircraft, Military Sealift Command controlled or arranged sealift and Government controlled air or land transportation.

**Department of Defense**. The Office of the Secretary of Defense (OSD) (including all boards, councils, staffs, and commands), DoD agencies, and the Departments of Army, Navy, and Air Force (including all of their activities).

**Derivative Classification**. A determination that information is in substance the same as information currently classified and the application of the same classification markings. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not posses original classification authority. Persons who apply derivative classification marking shall observe and respect original classification decisions and carry forward to any newly created documents any assigned authorized markings.

**Document**. Any recorded information, regardless of its physical form or characteristics, including, without limitation, written or printed matter, tapes, charts, maps, paintings, drawing, engravings, sketches, working notes and papers; reproductions of such things by any means or process; and sound, voice, magnetic, or electronic recordings in any form.

**Downgrade**. A determination that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect a lower degree of protection.

**Effectively Owned or Controlled**. A foreign government or any entity controlled by a foreign government has the power, either directly or indirectly, whether exercised or exercisable, to control the electron, appointment or tenure of the Offeror’s officers, or a majority of the Offeror’s board of directors by any means; e.g., ownership, contract, or operation of law (or equivalent power for unincorporated organizations).

**Embedded System**. An AIS that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem such as, ground support equipment, flight simulators, engine test stands, or fire control systems.

**Entity**. Any U.S. or foreign person.

**Electronic Questionnaire for Investigation Processing (e-QIP).** e-QIP is a secure website designed to process and store all personnel investigative forms for DoD, and are digital versions of the SF-86, SF-85P, and the SF-85.

**Escort**. A cleared employee, designated by the contractor, who accompanies a shipment of classified material to its destination. The classified material does not remain the personal possession of the escort but the conveyance in which the material is transported remains under the constant observation and control of the escort.

**Evaluated Products List**. A documented inventory of equipment’s, hardware software, and/or firmware that have been evaluated against the evaluation criteria found in DoD 5200.28-STD.

**Facility.** A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined herein.) For purposes of industrial security, the term does not include Government installations.

**Facility (Security) Clearance**. An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

**Firmware**. A method of organizing control of an AIS in a microprogrammed structure in addition to, or rather than, software or hardware. Microprograms are composed of microinstructions, normally resident in read-only memory, to control the sequencing of computer circuits directly at the detailed level of the single machine instruction.

**Foreign Government**. Any national governing body organized and existing under the laws of any country other than the United States and its possessions and trust territories and any agent or instrumentality of that government.

**Foreign Government Information**. Information that is: a) Provided to the U.S. by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or b) Produced by the U.S. pursuant to, or as a result of, a joint arrangement with a foreign government or governments, an international organization of governments or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence.

**Foreign Interest** Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than the U.S. or its possessions and trust territories, and any person who is not a citizen or national of the United States.

**Foreign Nationals** Any person who is not a citizen or national of the United States.

**Foreign Person**. A foreign government or international organization, to whom the U.S. is providing classified material.

**Formerly Restricted Data.** Classified information jointly determined by the DOE and its predecessors and the DoD to be related primarily to the military utilization of atomic weapons and removed by the DOE from the Restricted Data category pursuant to section 142(d) of the Atomic Energy Act of 1954, as amended, and safeguarded as National Security Information, subject to the restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.

**Freight Forwarder (Transportation Agent).** Any agent or facility designated to receive, process, and transship U.S. material to foreign recipients. In the context of the NISPOM, an agent or facility cleared specifically to perform these functions for the transfer of U.S. classified material to foreign recipients.

**Government-To-Government Channels**. Transfers by government officials through official channels or through other channels specified by the governments involved.

**Government Contracting Activity**. An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.

**Hand-Carrier**. A cleared employee, designated by the contractor, who occasionally hand-carries classified material to its destination in connection with a classified visit or meeting. The classified material remains in the personal possession of the hand-carrier except for authorized overnight storage.

**Home Office Facility**. The headquarters facility of a multiple facility organization.

**Independent Research and Development.** A contractor funded research and development effort that is not sponsored by, ore required in performance of, a contract or grant that consists of projects falling with the areas of basic research; applied research; develop­ment; and systems, and other concept formulation studies.

**Industrial Security**. That portion of infor­mation security which is concerned with the protection of classified information in the custody of U.S. industry.

**National Industrial Security System (NISS).** The National Industrial Security System (NISS) deployed on Oct. 1, 2018, replacing Industrial Security Facilities Database (ISFD) and Electronic Facilities Clearance System (e-FCL), and is the DCSA System of Record for industrial security oversight accessible by Industry, Government, and DCSA personnel. [ttps://ncaiss.dss.mil/](https://ncaiss.dss.mil/)

**Information**. Any information or material, regardless of its physical form or characteristics.

**Information Security**. The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order.

**Information System Security Officer**. The contractor employee responsible for the implementation of Automated Information Systems security, and operational compliance with the documented security measures and controls, at the contractor facility.

**Intelligence**. Intelligence is the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information, that concerns one or more aspects of foreign nations or of areas of foreign operations, and that is immediately or potentially significant to military planning and operations.

**Intelligence Information**. Information that is under the jurisdiction and control of the Director of Central Intelligence or a member of the Intelligence Community.

**Intelligent Terminal**. An AIS term that means a terminal that is programmable, able to accept peripheral devices, able to connect with other terminals or computers, able to accept additional memory, or which may be modified to have these characteristics.

**Joint Verification System (JVS).** Is a government established on-line database for keeping track of the status of both government and industry personnel with access to classified material and to what level access has been granted.

**Letter of Consent**. The form used by the CSA to notify a contractor that a PCL or a Limited Access Authorization has been granted to an employee.

**Letter of Offer and Acceptance (LOA)**. United States Department of Defense Offer and Acceptance that, when executed, provides that the U.S. offers to sell, subject to terms and conditions contained therein, defense material to a foreign government, and the foreign government accepts the offer, subject to those terms and conditions.

**Limited Access Authorization**. Security access authorization to CONFIDENTIAL or SECRET information granted to non-U.S. citizens requiring such limited access in the course of their regular duties.

**Military Export Sales**. Military Export Sales may by divided into Foreign Military Sales (FMS) under the AECA, sales under Section 607 of the Foreign Assistance Act (FAA) and Direct Commercial Sales. FMS and FAA are government-to-government transactions. For these sales, the DoD purchases articles and services from U.S. firms, takes title to the equipment, or has title to the articles to be sold from U.S. stocks, and sells the articles or services to the foreign buyer. For direct commercial sales, the U.S. firm sells directly to the foreign government or international organization.

**Material**. Any product or substance on, or in which, information is embodied.

**Multiple Facility Organization**. A legal entity (single proprietorship, partnership, association, trust, or corporation) that is composed of two or more facilities.

**National of the United States**. A national of the United States is: a) A citizen of the United States, or, b) A person who, though not a citizen of the United States, owes permanent allegiance to the United States.

***Note:*** *8 U.S.C. 1101(a) (22). 8 U.S.C. 1401, subsection (a) lists in paragraphs (1) through (7) categories of persons born in and outside the United States or its possessions who may qualify as nationals of the United States. This subsection should be consulted when doubt exists as to whether or not a person can qualify as a national of the United States.*

**National Security**. The national defense and foreign relations of the United States.

**National Security Information**. Any informa­tion that has been determined, pursuant to E.O. 12356 or any predecessor order, to require protection against unauthorized disclosure and is so designated. The classifications TOP SECRET, SECRET, and CONFIDENTIAL are used to designate such information and it is referred to as ‘‘classified information.’’

**NATO Information**. Information bearing NATO markings, indicating the information is the property of NATO, access to which is limited to representatives of NATO and its member nations unless proper NATO authority has been obtained to release outside of NATO.

**Need-to-Know**. A determination made by the possessor of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the classified information to perform tasks or services essential to the fulfillment of a classified contract or program.

**Network**. An AIS term meaning a network composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

**Original Classification**. An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required. (Only government officials, who have been designated in writing, may apply an original classification to information.)

**Parent Corporation**. A corporation that owns at least a majority of another corporation’s voting securities.

**Personnel (Security) Clearance**. An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

**Possessions**. U.S. possessions are the U.S. Virgin Islands, Guam, American Samoa, Swain’s Island, Howland Island, Baker Island, Jarvis Island, Midway Islands (this consists of Sand Island and Eastern Island), Kingman Reef, Johnston Atoll, Navassa Island, Swan Island, Wake Island, and Palmyra Island.

**Prime Contract**. A contract by a GCA to a contractor for a legitimate government purpose.

**Prime Contractor**. The contractor who receives a prime contract from a GCA.

**Principal Management Facility**. A cleared facility of an MFO which reports directly to the HOF and whose principal management official has been delegated certain personnel security administration responsibilities for a defined geographical or functional area. The PMF will function as a HOF in relation to its area of responsibility. Both cleared and uncleared facilities may be under the jurisdiction of a PMF.

**Proscribed Information.**

a. Top Secret information;

b. Communication Security (COMSEC) information, except classified keys used to operate secure telephone units (STU IIIs);

c. Restricted Data as defined in the U.S. Atomic Energy Act of 1954, as amended;

d. Special Access Program (SAP) information; or

e. Sensitive Compartmented Information (SCI).

**Protective Security Service**. A transportation protective service provided by a cleared commercial carrier qualified by the Military Traffic Management Command (MTMC) to transport SECRET shipments.

**Public**. Any contractor, subcontractor, Government official, or other individual who does not require access to information (classified or unclassified) in furtherance of the performance of the classified contract under which the information was provided to the contractor or as authorized by the NISPOM.

**Public Disclosure**. The passing of information and/or material pertaining to a classified contract to the public, or any member of the public, by any means of communication.

**Reference Material**. Documentary material over which the GCA, who lets the classified contract, does not have classification jurisdiction, and did not have classification jurisdiction at the time the material was originated. Most material made available to contractors by the Defense Technical Information Center and other secondary distribution agencies is reference material as thus defined.

**Regrade**. To assign a higher or lower security classification to an item of classified material.

**Remote Terminal**. A device for communication with an automated information system from a location, that is not within the central computer facility.

**Representative of a Foreign Interest (RFI).** A citizen or national of the United States, who is acting as a representative of a foreign interest. (See ‘‘Foreign Interest.’’)

**Restricted Area**. A controlled access area established to safeguard classified material, that because of its size or nature, cannot be adequately protected during working hours by the usual safeguards, but that is capable of being stored during non-working hours in an approved repository or secured by other methods approved by the CSA. (See paragraph 5-305 of the NISPOM.)

**Restricted Data**. All data concerning the design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the RD category pursuant to section 142 of the Atomic Energy Act of 1954, as amended.

**SECRET**. The designation that shall be applied only to information of material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

**Security Cognizance**. The Government office assigned the responsibility for acting for CSAs in the discharge of industrial security responsibilities described in the NISPOM.

**Security in Depth**. A determination made by the CSA that a contractor’s security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility.

**Security Violation**. Failure to comply with the policy and procedures established by the NISPOM that reasonably could result in the loss or compromise of classified information.

**Sensitive Compartmented Information**. All Intelligence Information and material that requires special controls for restricted handling within Compartmented channels and for which compartmentation is established.

**Shipper**. One who releases custody of material to a carrier for transportation to a consignee. (See ‘‘Consignor.’’)

**Short Title**. An identifying combination of letters and numbers assigned to a document or equipment for purposes of brevity.

**Source Document** A classified document, other than a classification guide, from which information is extracted for inclusion in another document.

**Special Access Program**. Any program that is established to control access, distribution, and to provide protection for particularly sensitive classified information beyond that normally required for TOP SECRET, SECRET, or CONFIDENTIAL information. A Special Access Program can be created or continued only as authorized by a senior agency official delegated such authority pursuant to E.O. 12356.

**Standard Practice Procedures**. A document(s) prepared by a contractor that implements the applicable requirements of the NISPOM for the contractor’s operations and involvement with classified information at the contractor’s facility.

**Subcontract**. Any contract entered into by a contractor to furnish supplies or services for performance of a prime contract or a subcontract. For purposes of the NISPOM a subcontract is any contract, subcontract, purchase order, lease agreement, service agreement, Request for Quotation (RFQ), Request for Proposal (RFP), Invitation for Bit (IFB), or other agreement or procurement action between contractors that requires or will require access to classified information to fulfill the performance requirements of a prime contract.

**Subcontractor**. A supplier, distributor, vendor, or firm that furnishes, supplies or services to or for a prime contractor or another subcontractor, who enters into a contract with a prime contractor. For purposes of the NISPOM, each subcontractor shall be considered as a prime contractor in relation to its subcontractors.

**Subsidiary Corporation**. A corporation in which another corporation owns at least a majority of its voting securities.

**System Software**. Computer programs that control, monitor, or facilitate use of the AIS; for example, operating systems, programming languages, communication, input-output control, sorts, security packages and other utility-type programs. Considered to also include off-the-shelf application packages obtained from manufacturers and commer­cial vendors, such as for word processing, spreadsheets, database management, graphics, and computer-aided design.

**Technical Data**. Information governed by the International Traffic in Arms Regulation (ITAR) and the Export Administration Regulation (EAR). The export of technical data that is inherently military in character is controlled by the ITAR, 22 CFR 120.1-130.17 (1987). The export of technical data that has both military and civilian uses is controlled by the EAR, 15 CFR 368.1-399.2 (1987).

**TOP SECRET**. The designation that shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

**Transclassification**. When information has been removed from the RD category by a joint determination of DOE and DoD and placed in the FRD category in accordance with section 142d of the Atomic Energy Act.

**Transmission**. The sending of information from one place to another by radio, microwave, laser, or other non-connective methods, as well as by cable, wire, or other connective medium. Transmission also includes movement involving the actual transfer of custody and responsibility for a document or other classified material from one authorized addressee to another.

**Transshipping Activity**. A government activity to which a carrier transfers custody of freight for reshipment by another carrier to the consignee.

**United States and Its Territorial Areas**. The 50 states, the District of Columbia, the Commonwealth of Puerto Rico, Guam, American Samoa, the Virgin Islands, the Trust Territory of the Pacific Islands (also called Micronesia), Midway Island, Wake Island, Johnston Atoll, Kingman Reef, Swain’s Island, and Palmyra Island.

**Unauthorized Person**. A person not authorized to have access to specific classified information in accordance with the requirements of the NISPOM.

**United Sates**. The 50 states and the District of Columbia.

**United States Citizen (Native Born)**. A person born in one of the following locations is considered to be a U.S. citizen for industrial security purposes: the 50 United States; District of Columbia; Puerto Rico; Guam; American Samoa; Northern Mariana Islands; U.S. Virgin Islands; Panama Canal Zone (if the father or mother (or both) was, or is, a citizen of the U.S.); the Federated States of Micronesia; and the Republic of the Marshall Islands.

**U.S. Person**. Any form of business enterprise or entity organized, chartered or incorporated under the laws of the United States or its possessions and trust territories and any person who is a citizen or national of the United States.

**Upgrade**. A determination that certain classified information, in the interest of national security, requires a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a higher degree.

**Voting Securities**. Any securities that presently entitle the owner or holder thereof to vote for the election of directors of the issuer or, with respect to unincorporated entities, individuals exercising similar functions.

**Working Hours**. The period of time when:

a. There is present in the specific area where classified material is located, a work force on a regularly scheduled shift, as contrasted with employees working within an area on an overtime basis outside of the scheduled workshift; and

b. The number of employees in the scheduled work force is sufficient in number and so positioned to be able to detect and challenge the presence of unauthorized personnel. This would, therefore, exclude janitors, maintenance personnel, and other individuals whose duties require movement throughout the facility.