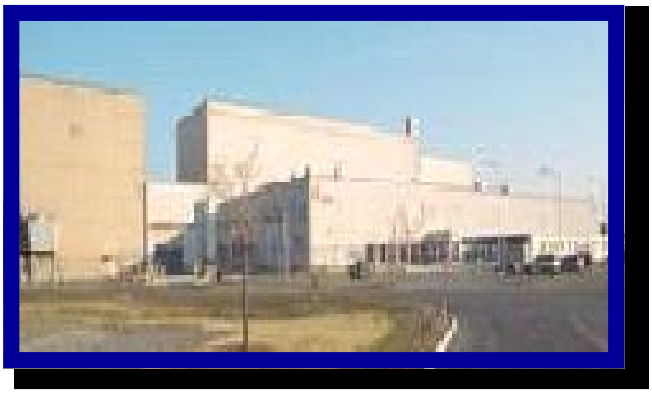
ITT

ITT Corporation
Space Systems Division
Rochester, NY &
Bloomfield, NJ

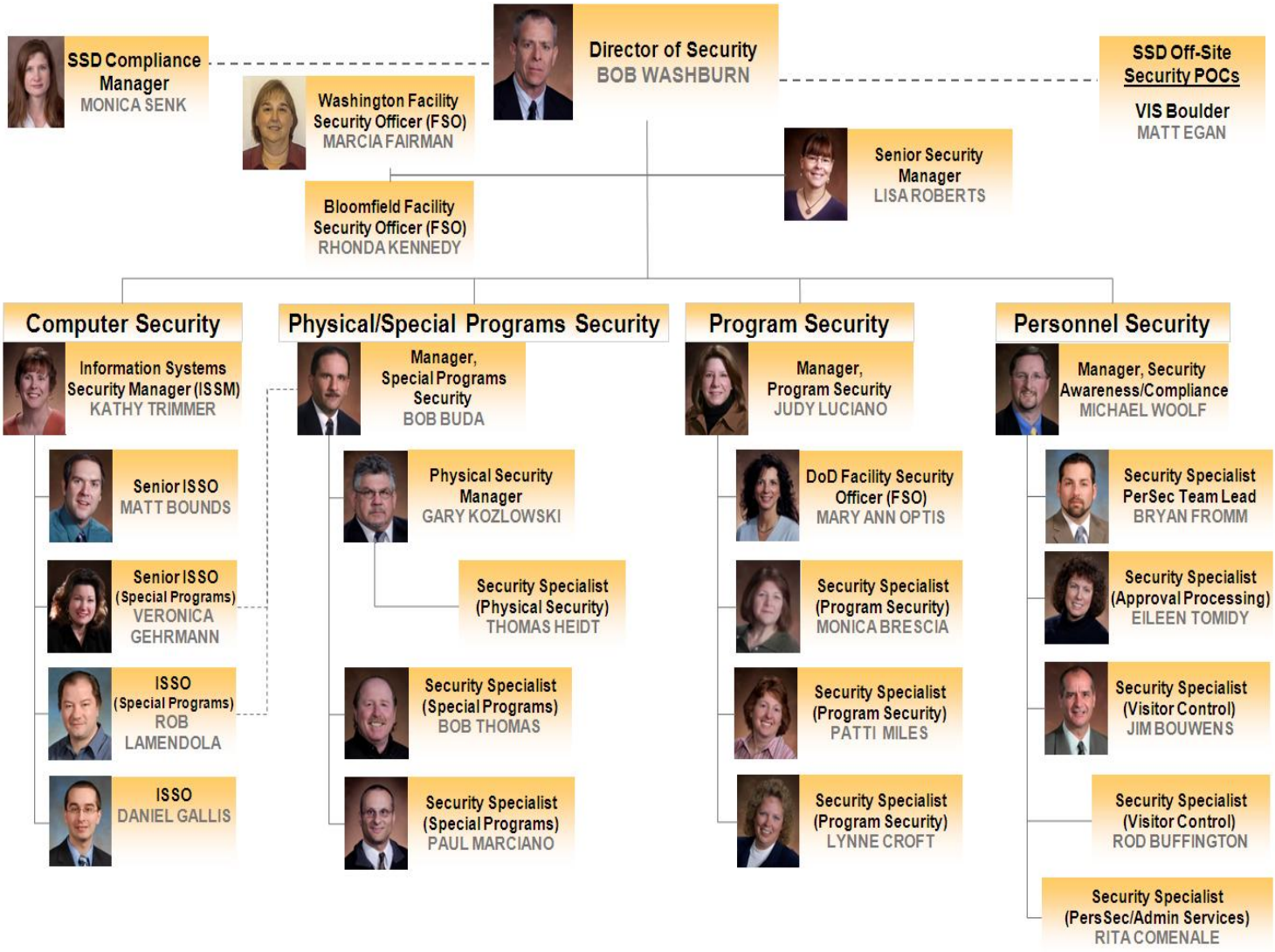


Employee Security Handbook
"Your Secrets to Success"

Updated: 12/03/09

Table of Contents

Table of Contents



Introduction

"This handbook is designed to provide you with a basic understanding of the various security policies and procedures and direct you where to find more detailed information about security as necessary. It will also describe your role and responsibilities as they pertain to security and the protection of classified government information and attempt to answer some basic questions you may have about those responsibilities. This "virtual" handbook allows SSD Security to be proactive and responsive in updating or modifying our policies and procedures as needed to better align ourselves with ever-changing government and customer regulations as well as to better serve the needs of our internal customers (YOU) as SSD continues to evolve and encounters new business challenges.

All official SSD Security policies and procedures may be found in the Command Media Library under the Resource Management folder in the 1600 number series.

In today's environment, change is continuous. If you have any questions regarding security or the information in this handbook, please contact any of the security professionals in your Space Systems Division Security Office for clarification."

Robert "Bob" Washburn
ITT Corporation, Space Systems Division
Director of Security
Commercial: (585) 269-5578
Secure: 815-3479

SSD Security Phone Directory

Name	Title	Location	Phone	Secure	Pager	Cell
Director & Supervisory Staff						
Washburn, Bob	Director of Security	3/11/HE-37220	269-5578	815-3479	521-0129	
Roberts, Lisa	Senior Security Manager	3/11/HE-37220	269-5855	815-3350	521-9858	905-9748
Buda, Robert	Manager, Physical Security, Special Program Security & COMSEC	1-601-KP 25114	269-7024	817-7460	521-5138	797-3265
Luciano, Judy	Manager, Program Security	1/6/RTP-39600	269-7391	815-3582	521-5236	
Trimmer, Kathy	Mgr, Information Systems Security (ISSM)	1/101/RTP-39500	269-7711	815-3768	521-9975	
Woolf, Michael	Mgr, Security Awareness/Compliance	3/11/HE-37220	269-5363	815-3411	521-0241	(202) 375-4718
Rochester-Based Security Staff						
Bounds, Matthew	Senior ISSO / DoD ISSO	3/11/HE-37220	269-7640	815-3427	521-9997	
Bouwens, James	Security Specialist (Visits)	6/5/HE-37013	269-5167	815-3348		
Brescia, Monica	Program Security Specialist	3/11/HE-37220	269-5072	815-3353	521-0079	
Buffington, Rod	Security Specialist (Visits)	3/11/HE-37220				
Comenale, Rita	Security Specialist & Admin Services	3/11/HE-37220	269-5887			
Croft, Lynne	Security Specialist	1/6/RTP-39600	269-7400	815-3661		
Fromm, Bryan	Personnel Security Team Lead	4/5/HE Room	269-6824			
Gallis, Daniel	ISSO	3/11/HE-37220	269-6736	815-3401		
Gehrmann, Veronica	Senior ISSO, Special Programs	1-601-KP 25114	269-7008		521-5178	
Heidt, Thomas	Physical Security Specialist					
Kozlowski, Gary	Physical Security Manager	1/101-39500	269-5471	815-3585	521-4213	208-4219
Lamendola, D. Rob	ISSO (Special Programs)	3-11-HE-37220	269-7809		521-0019	
Marciano, Paul	Physical Security Specialist	1/101/RTP-39500	269-7392		521-5287	766-8088
Miles, Pattie	Security Specialist	1/101/RTP-39500	269-6971	815-3584		
Optis, Mary Ann	DoD Facility Security Officer	5/5/HE-37026	269-5120		N/A	683-4717
Thomas, Bob	Special Programs Security Specialist	1-601-KP 25114	269-7072		521-2389	
Tomidy, Eileen	Personnel Security Specialist	3/11/HE-37220	269-7708	815-3428		
Washington Facility Security Officer (Herndon, VA)						
Fairman, Marcia	12930 WorldGate Dr, Ste 500 Herndon, VA 20170		1624/1649 (SCIF) 703-668-3547	816-3501	(800) 204-1013	(703) 635-0617
Bloomfield Facility Security Officer (Bloomfield, NJ)						
Kennedy, Rhonda	1515 Broad St., Bldg. D Bloomfield, NJ 07003		(973) 284-5451		(888) 200-8804	
Guard on duty			TBD		(888) 200-8864	(973) 738-7567
Other ITT Value Center Sites supporting SSD Personnel:						
Egan, Matthew	**ITT VIS, Facility Security Officer**	4990 Pearl East Cir. Boulder, CO 80301	(303) 544-4430	Asst: Eva Barros (303) 684-4045		(202) 253-9759
Fallon, Mark	**ITT ES, Director of Security**	77 River Road Clifton, NJ 07014	(973) 284-4480	Asst: Rose Shumack (973) 284-4537		
Woenker, Jody	**ITT CS, Director of Security**	1919 W. Cook Rd. Fort Wayne, IN 46818	882-6927	Asst: Jamie Fuller 882-6762 Asst: Mike Ellsworth 882-7075		

GuardsMark Personnel				Miscellaneous Numbers		
Hargather, Doug	Supervisor	1-101-EP	269-6460	**HE Security Conf Rm**		815-3432
Eden, Alice Strassner, Sue	PassFab Office (#SSD-ITT-Pass-Fab)	1/601/KP-30150	269-6991	**Staff Meeting Meet Me #**		851-6338 PIN 569433
Guard on duty	Alarm Control Center	Bldg. 101	7349/7350/7351	**Faxes**	**UNCLAS Fax**	**Classified Fax**
Guard on duty	B101 Front Desk	Bldg. 101	269-7631/4631	**HawkEye**	**(585) 269-5655**	**(585) 342-8025**
Guard on duty	5th Floor Guard Post	HE	269-5390	**RTP-6**	**(585) 672-8042**	**(585) 269-5018**
Guard on duty	Visitor Lobby	HE	5610	**B101**	**None**	**(585) 269-6063**
Guard on duty	Visitor Lobby	Bldg. 601	6643	**Bldg. 601**	**None**	**(585) 269-7080**
Guard on duty	Visitor Lobby	RTP 6	5116	**Merrifield**	**(703) 342-1680**	**(703) 342-1651**
				Herndon SP Office	**(703) 668-3265**	**(703) 668-3265**

SSD Security CML Document Listing by Subject Area

CML Document #	Tier	Title
SSD-1600	1	Security Policies and Procedures
		Computer Security
SSD-1600-01	2	ITT-SSD Computer Security Policy for Secure Areas
ROC-1600-01-001	3	Data Transfer from Unclassified Network to ISNET
ROC-1600-01-002	3	Requesting Software Installs on ISNET
ROC-1600-01-003	3	Removing Data from ISNET
ROC-1600-01-003-01	4	Media Sanitization and Release Form
ROC-1600-01-004	3	Overnight Logon Violation Procedure
ROC-1600-01-005	3	Control of Portable Electronic Devices -ITT-SSD Secure Areas
ROC-1600-01-006	3	Digital Camera Use in ITT-SSD Secure Area's
ROC-1600-01-006-01	4	Digital Camera Briefing Statement
ROC-1600-01-007	3	Removing Computers from ITT-SSD Secure Areas
ROC-1600-01-007-01	4	Computerized Hardware Release Form
ROC-1600-01-008	3	Procedure for Non-ITT Computer Equipment Entering Secure Areas
ROC-1600-01-008-01	4	Non-ITT Computer Equipment Registration Form
ROC-1600-01-009	3	Requesting Software Installs on DoD Information Systems
ROC-1600-01-009-01	4	DoD Software Request Form
ROC-1600-01-010	3	Performing Trusted Downloads from DoD Information Systems
ROC-1600-01-010-01	4	DoD Trusted Download Form
ROC-1600-01-011	3	Requesting Logon Authorization in DoD Labs
ROC-1600-01-011-01	4	Logon Authorization Form for DoD Labs
WSH-1600-01-012	3	Data Transfer from Vienna Unclass Network to ISNET
ROC-1600-01-013	3	Data Transfer from Unclass to Special Programs
		Security Incident
SSD-1600-18	2	Security Incident Policy
SSD-1600-18-001	3	Security Incident Management Procedure
SSD-1600-18-001-01	4	Security Incident Statement
SSD-1600-18-001-02	4	Incident 24 Hour Notification
SSD-1600-18-001-03	4	Security Incident Report
SSD-1600-18-001-04	4	Portable Electronice Device (PED) Infraction Report Form
SSD-1600-18-001-05	4	Security Incident Investigation Checklist
SSD-1600-18-001-06	4	Inadvertent Disclosure Briefing Form
		Personnel Security
SSD-1600-19	2	Personnel Security Policy
SSD-1600-19-001	3	Procedure for Reporting Foreign Contact
SSD-1600-19-001-01	4	Foreign Contact Reporting Form
SSD-1600-19-002	3	Procedure for Reporting Foreign Travel
SSD-1600-19-002-01	4	Foreign Travel Reporting Form
SSD-1600-19-002-02	4	Foreign Travel Reporting (SUP)

SSD Security CML Document Listing by Subject Area

CML Document #	Tier	Title
Personnel Security (continued)		
SSD-1600-19-003	3	Procedure for Processing a Request for Security Clearance
SSD-1600-19-003-01	4	SAAR Form
SSD-1600-19-003-02	4	Counterintelligence Security Polygraph Form
SSD-1600-19-004	3	Process for Outgoing Classified Visits
SSD-1600-19-004-01	4	ITT SSD Travel Request Form
SSD-1600-19-005	3	Pre-Briefing Review
SSD-1600-19-005-01	4	Pre-Briefing Checklist
SSD-1600-19-006	3	Personnel Security Reporting Requirements
SSD-1600-19-006-01	4	Personnel Security General Report Form
SSD-1600-19-006-02	4	Personnel Security Marriage/Cohabitation Update Form
SSD-1600-19-007	3	Procedure for Executing an SSD Security NDA
SSD-1600-19-007-01	4	SSD Security Non-Disclosure Agreement Form
Security Operations		
ROC-1600-20	2	Security Operations Policy
ROC-1600-20-001	3	Visitor Access Badge Procedures
ROC-1600-20-001-01	4	Portable Electronic Device (PED) Visitor Briefing
ROC-1600-20-002	3	ITT-SSD Badge Issue (future document)
ROC-1600-20-003	3	Image and Audio Capturing On-site
ROC-1600-20-004	3	Lost and Found Property
ROC-1600-20-005	3	Non-Government Material Removal
ROC-1600-20-005-01	4	Material Removal Pass
ROC-1600-20-006	3	Control of Classified Material in an Emergency (future document)
ROC-1600-20-007	3	Transmittal of Classified Information and Material
ROC-1600-20-007-01	4	Request for Shipment Form
ROC-1600-20-007-03	4	Courier Instructions and Guidelines (future document)
ROC-1600-20-008	3	Furniture and Container Removal from Secure Areas
ROC-1600-20-008-01	4	Security Check Request for SCIF to Non-SCIF Move
ROC-1600-20-009	3	Interplant Deliveries via Courier
ROC-1600-20-009-03	4	Long Term Visitor Agreement (formerly ROC-1600-03-001-02)
WSH-1600-20-010	3	WSH Opening/Closing Procedures for SCIF
ROC-1600-20-011	3	Fascimile Process
ROC-1600-20-011-01	4	Fascimile Form
ROC-1600-20-012	3	Hardcopy Review Procedure (future document)
Security Compliance		
SSD-1600-21	2	Information Security Laptop Computer Security Policy (future document)

Personnel Security

Personnel Security is the security discipline that deals with all of the security functions that involve people and the granting of or continuing access to classified government information and material. This section contains the basic information about personnel security that you should be aware of.

Clearance Process

An employee who needs access to classified material to do their job must go through the clearance submission process. The existing SSD clearance process is established per requirements specified by our government customers. A detailed description of the process, procedures and forms to be filled out are located in the SSD-1600-19-003 number series of the Command Medial Library.

Citizenship Requirement

Individuals must be United States citizens in order to be processed for a security clearance or access approval. Proof of citizenship is required.

Background Investigation

The security clearance submission process requires that the employee submit a personal history report covering up to the last ten years of their life (depending on the level of access needed). Once the history report is submitted, the government will conduct a Single-Scope Background Investigation (SSBI) or a lesser investigation (as needed). The background investigation consists of an in-depth check of local and national databases, the employee's past residences, employment, school history, medical history, and interviews of the employee and people they have associated with in the past several years.

Adjudicative Review Process

Once an individual has had a Background Investigation completed on them, they will undergo adjudication. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, are considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator will consider the following factors:

a. Nature, extent, and seriousness of the conduct;
b. Circumstances surrounding the conduct, to include knowledgeable participation;
c. Frequency and recentness of the conduct;
d. Individual's age and maturity at the time of the conduct;
e. Voluntariness of participation;
f. Presence or absence of rehabilitation and other pertinent behavioral changes;
g. Motivation for the conduct;
h. Potential for pressure, coercion, exploitation, or duress; and
i. Likelihood of continuation or recurrence.

Each individual's case will be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security.

13 Adjudicative Guidelines

When making a decision on whether to grant or continue eligibility for a security clearance for an individual, the government adjudicator makes an overall determination to decide whether granting or continuing eligibility is clearly consistent with the interests of national security. The adjudicator makes this determination based upon careful consideration of the 13 Adjudicative Guidelines listed below using the whole person concept.

Guideline A: Allegiance to the United States
Guideline B: Foreign influence
Guideline C: Foreign preference
Guideline D: Sexual behavior
Guideline E: Personal conduct
Guideline F: Financial considerations
Guideline G: Alcohol consumption
Guideline H: Drug involvement
Guideline I: Emotional, mental, and personality disorders
Guideline J: Criminal conduct
Guideline K: Security violations
Guideline L: Outside activities
Guideline M: Misuse of information technology systems

> ***Note:*** *SSD Security can, upon request, provide more specific information on each of the above categories along with the mitigating factors associated with each.*

Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding the whole person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator will consider whether the person:

a. Voluntarily reported the information;
b. Was truthful and complete in responding to questions;
c. Sought assistance and followed professional guidance, where appropriate;
d. Resolved or appears likely to favorably resolve the security concern;
e. Has demonstrated positive changes in behavior and employment;
f. Should have his or her access temporarily suspended pending final adjudication of the information.

If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

Personnel Security

Access vs. Clearance

An individual that has been favorably adjudicated and approved for access to classified information and material has officially been granted either a "security clearance" or "access approval" and will undergo indoctrination and receive their initial security brief. Below is a brief description of the difference between a security clearance and an access approval.

- A Department of Defense (DoD) clearance is:
  - Overt (i.e. openly acknowledged),
  - Granted under the authority of the Secretary of Defense, and
  - Allows access to *Department of Defense* classified information based on your need -to-know.
- Access approvals are:
  - Granted under the authority of the Director of Central Intelligence, and
  - May be overt or covert (i.e. hidden, secret, unacknowledged)
  - Allows access to classified *intelligence* information based on your need-to-know.

Access Termination or Suspension

An individual that has been favorably approved and indoctrinated for access to classified program information and material will retain that access until it is determined that they no longer need it to do their job. When this happens either the individual or their supervisor should contact SSD Security to arrange for a **debriefing**. A debriefing is a set of final instructions and guidelines given to remind formerly-cleared individuals of their continuing obligation to protect classified information. Events that cause an individual to be debriefed include:

- When the need for access to classified information is no longer required (e.g. conclusion, loss of, or removal from a classified contract and no other contract is available);
- Unauthorized travel to a criteria country;
- Periods of extended absence from work (e.g. medical reasons or schooling); or
- Termination of employment.

An employee's access may also be temporarily suspended for some of the above or other reasons. Suspending an employee's access is rare and usually done temporarily (less the 90 days) for disciplinary reasons at the request of the government pending special inquiries for reasons that would be explained to the employee via private communication.

Access Reinstatement

An employee whose access has been suspended or terminated may have their access reinstated fairly easily. For example, an employee gets debriefed at the conclusion of a classified contract because another one isn't available at the time. A few months later the same employee may be reinstated when a new classified contract begins or has a space available for them. Another example is an employee who has their access terminated upon leaving employment with one company and then has it reinstated a short time later after beginning employment with a new company. Unless the government has revoked the employee's approval for some reason. The reinstatement process may be fairly quick if the new contract or employment is with the same approving agency. If the new contract or employment is with a different agency, a "crossover process" is done which takes somewhat longer. In some cases, the government uses a Time Accounting (TA) procedure to thoroughly check an inactive individual's personnel and other records to determine if the subject's PSQ has changed since last briefed. For the TA procedure to be used, the subject must:

- Have a current Single Scope Background Investigation within the last five (5) years
- Be debriefed or inactive, and
- The debriefing or period of inactivity is less than one (1) year.

or

- Has a current Single Scope Background Investigation within the last one (1) year,
- Was approved for access but never briefed,

or

- Was debriefed within the past year (inactive).

or

- Has a current Single Scope Background Investigation within the last five (5) years

and

- Has changed companies.

Individual Reporting Requirements & Responsibilities

As a cleared individual who accepts responsibility for access to classified information, you will be required by law to report certain information to the government via your SSD Security Office. The things you must report consist of personal history changes and events as well as professional information and events about yourself or about other cleared individuals that you witness or become aware of. Some examples of both are as follows:

Personal Information and Life Occurrences

You are required to report any events or activities that could have an impact on the status of your personnel security clearance or access approval to include:

- Any change in name.
- Any change in marital status.
- Any change in citizenship.
- Any police involvement and legal proceedings.
- Any sudden financial affluence or excessive debt.
- Any professional mental health counseling.
- Any foreign travel, including Canada (SSD-1600-19-002).
- Continuing contact with a foreign national (SSD-1600-19-001).
- If you become a representative of a foreign interest (RFI) or if your status as an RFI is materially changed. (An RFI refers to your susceptibility for influence by any foreign individuals, companies, or governments through personal, professional, or business relationships.)
- Any contact by another individual which suggests that you may be the target of an attempted exploitation by the intelligence services of another country.

Professional Information & Events You Witness or Become Aware of

- Any events that affect the proper safeguarding of classified information or violate established security protocols (i.e. security incidents).
- Any information that indicates classified information has been or may have been lost or compromised.
- Any confirmed loss, compromise or suspected compromise of classified information, foreign or domestic. Material that cannot be located within a reasonable period of time shall be presumed to be lost until an investigation determines otherwise.
- Information concerning actual, probable or possible espio-

nage, sabotage, or subversive activities.

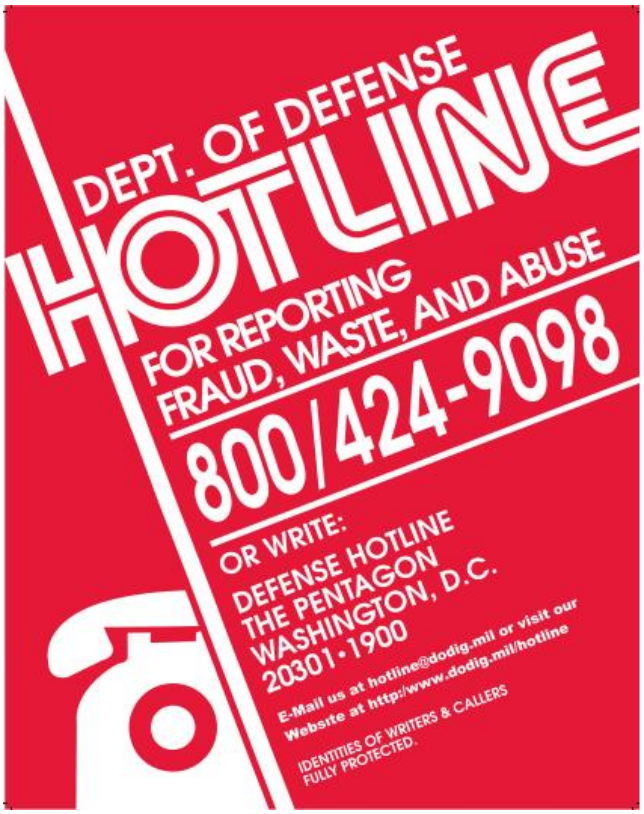
- Efforts by any individual to obtain illegal or unauthorized access to classified information or to compromise a cleared employee.
- Adverse information concerning any cleared employee.
- Any mis-use of government or company information technology (IT) systems.
- Receipt of classified information via unauthorized channels (e.g. company mail).
- Any pre-contract negotiation or award not placed through the government that involves, or may involve:
    1) The release or disclosure of U.S. classified information to a foreign interest, or
    2) Access to classified information furnished by a foreign interest.
- Any events that could have an impact on the status of our facility clearance.
- When you no longer require access to classified information.
- If you no longer wish to be processed for a clearance/access or continue an existing clearance or access.
- Termination of employment.
- The death of a cleared employee.

Where to Report

You may report any and all security concerns to:

- Your SSD Security Staff.
- You may also report DoD security concerns and Fraud, Waste and Abuse regarding work done on a government contract to the DoD Hotline by phone, email, or on the web.

WARNING: *Do NOT disclose classified information when reporting via one of the DoD Hotline methods!*



Personnel Security

Required Security Training and Briefings

There are periodic training requirements that SSD as an organization and you as a cleared individual must adhere to. The more common requirements are listed below.

Initial Security Briefing

Prior to being granted access to classified information, an employee will receive an initial security briefing that includes an overview of the security system, the employee's reporting obligations and requirements, and general SSD security procedures. Conveying security information and duties specific to the employee's job is the responsibility of the employee's supervisor.

Refresher Briefing

It is a government requirement that a refresher briefing be conducted, as a minimum, annually which reinforces the information provided during the initial briefing and informs employees of relevant changes in security regulations.

Courier Briefing

Prior to being granted authorization to hand-carry any classified material outside of an SSD SCIF you must first go to your local security office to receive a courier briefing.

Escort Briefing

Prior to being authorized to escort un-cleared individuals within an SSD SCIF, you must first go to your local security office and receive an escort briefing.

Defensive Security Travel Briefing

Given to travelers to countries that may be hostile to Americans or foreigners to make them aware of personal safety or counterintelligence threats and to suggest ways to avoid being targeted.

International Travel to High Risk Areas

All ITT employees intending to travel to a "high-risk" area must have their travel approved by the ITT Defense President prior to leaving. The list of countries, specific procedures and form for requesting travel to a high-risk area are located on the ITT Corporate Security web page at: http://info.itt.com/security/.

Debriefing

Cleared employees will be debriefed:

- At time of termination of employment (discharge, resignation, or retirement),

or

- When access to classified information is no longer required,

or

- When an employee's clearance or access is terminated, suspended, or revoked.

Visit Certifications

Outgoing Visitors

You may occasionally need to have proof of your clearance/access forwarded to another facility in order to conduct business there at the classified level. CML document series ROC-1600-19 provides detailed information on how employees and other individuals with SSD-sponsored security clearances/access approvals can have their information sent to other companies or organizations for meetings, conferences, etc..

Requests to have your clearance sent to another location should be done as far in advance as possible to allow SSD Security to address any problems that may arise to ensure you are not delayed upon your arrival. Please submit 3-5 days prior to initiating any travel within the United States and 7-10 days for travel outside of the United States.

It is vital that you supply ALL information on the travel request form, especially the point of contact's telephone number and city/state or country where the facility is located.

Visit certifications may be arranged for up to twelve-month periods. This is known as a "Long-Term Certification" or "Permanent Certification" and is convenient when an individual anticipates making multiple visits to a location over a period of time.

Incoming Visitors

If you are hosting an incoming visitor or visitors to any ITT SSD facility, you must ensure a Visit Request is submitted via the Lotus Notes database. If you do not have access to Lotus Notes, please ask the administrative assistant for your work area who should be able to assist you.

If access to any of our Secure Areas is needed during the visit, then the incoming individual's security office must pass their clearance/access approval data to SSD Security Visitor Control. SSD's visitor control specialist is **Jim Bouwens** who can be reached at (585) 269-5167 (open) or 815-3348 (secure). **Please note that SSD Security *will not* request certifications for incoming visitors!** Incoming certifications may be sent as indicated below.

Rochester	**SCI Visits**	**DoD Visits**
Email:	ittssd-visit@itt.npa.gov (CWAN/GWAN)	ssd-visit@itt.com (open)
Facsimile:	(585) 342-8025 (Secure STU-III)	(585) 269-5655 (open)
JPAS SMO Code:	30KA0 (via Level 3 or lower)	30KA0 (via Level 5 or higher)

Washington	**SCI Visits**	**DoD Visits**
Email:	ittssd-visit@itt.npa.gov (CWAN/GWAN)	ssd-visit@itt.com (open)
Facsimile:	(703) 342-1651 (Secure STU-III)	(703) 342-1680 (open)
JPAS SMO Code:	3GEJ8 (via Level 3 or lower)	3GEJ8 (via Level 5 or higher)

Bloomfield	**SCI Visits**	**DoD Visits**
Email:	N/A	ssd-visit@itt.com (open)
Facsimile:	N/A	_____(open)
JPAS SMO Code:	N/A	_____ (via Level 5 or higher)

Physical Security

Physical Security refers to the equipment, personnel and methods used to control and prevent unauthorized access to our facilities in the protection of SSD employees and associates, company proprietary information, export controlled information, and U.S. government national security information. Physical Security includes:

1) equipment (e.g. cameras, sensors, alarms, etc.);
2) personnel (e.g. guards);
3) materials (ID badges and badge readers); and of course
4) special policies and procedures.

There are a few different types of secure facilities at SSD but the most common ones are Sensitive Compartmented Information Facilities (SCIFs) and DoD Secure Areas. As a cleared individual, you must be aware of physical security policies and procedures you must adhere to. This section describes the most common ones you must be familiar with although certain areas or facilities may have additional, more restrictive guidelines.

Badge Recognition

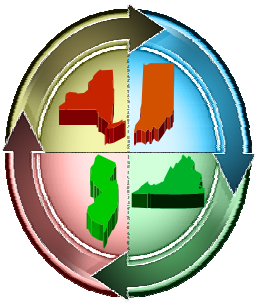
ITT Defense Identification Badges

SSD ID Badges are made in accordance with an established ITT Defense standard. This means that if an employee from another ITT Defense Value Center visits us or if you go to another ITT Defense Value Center you can tell what type of security clearance/access each other has. The examples on the right depict the standard badge and the type of security clearance indicated for each.

Badge Reciprocity between ITT SSD and Tenant Facilities

Although your ITT Corporate badge is of a standard design, in order to be recognized at all ITT Value Centers, each Value Center manages its badge system independently. Although it is possible to synchronize employee badge data between value centers, it would be manpower and cost intensive and basically not a sound practice for good security. Therefore, the following badge reciprocity guidelines have been established between ITT SSD, CS & ES/EW Security:

- Badges issued by CS and ES to SSD employees will automatically be synchronized with SSD and will work at all SSD facilities.
- Badges issued by SSD will only work at CS or ES if the employee requests it and has a genuine need to visit there.

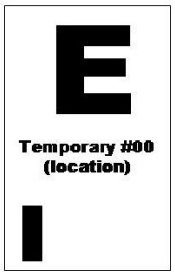


- Rochester employees needing their badges to work at ITT CS or ES may Contact Security PassFab at 585-269-6991 (SSD-ITT-PassFab@itt.com) and request it on an individual basis.
- Employees at ITT CS needing their badges to work at ITT ES and vice versa must also contact Security PassFab as indicated above and request it on an individual basis.

SSD Secure Area Badge

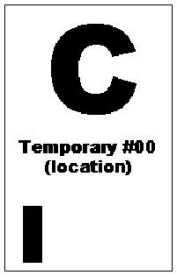
The reverse side of the standard ITT Defense ID badge for employees with SCI access will look similar to the image on the right. The various colored stripes on the badge indicate the different programs and/or levels of program access the bearer has. The vast majority of SSD employees with one of these badges will have a single black stripe which indicates SCI access at the SI/TK level. If other stripes are present they will be of varying colors or may have a number on them to indicate additional program accesses. If there is a half-stripe present, then the bearer has limited access to the particular program.

"E" Badge



E-badges are temporary badges provided to employees who have misplaced or forgotten their SCIF badge. E badges are issued with a PIN and allow access to all of SSD's perimeter doors in addition to our SCIF doors.

"C" Badge



These badges are issued to **cleared visitors/customers who have had their clearances passed** to us in advance so that they may enter our SCIF to hold classified discussions. C-badges **do not allow unescorted access** through any of SSD's SCIF or perimeter doors. See CML Policy ROC-1600-19 for the different methods of receiving visit certifications.

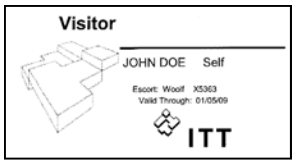
"ITAR" Badge

ITAR badges allow proximity access to all of SSD's exterior doors and are only issued to verified "U.S. persons.". A "U.S. person" is defined as a U.S. citizen or an alien with a valid U.S. Permanent Resident Identification (Green Card). CML policy ROC-1600-20-001 pertains. The ITAR badge may be issued to the following:

1) Cleared or non-cleared SSD employees who have forgotten, misplaced, lost, etc. their picture badge or haven't been issued one yet and need routine access to non-classified SSD areas.
2) Cleared or non-cleared ITT employees from other ITT Defense Value Centers when they are working with SSD on a contract and need regular access to non-cleared office areas.
3) Visitors that will need frequent and repeated unrestricted access to our non-cleared areas over a limited period of time for such reasons as facilities work or sub-contract work.

Visitor Badges

Short-term visitors that have verified their U.S. person status but do not need access to ITAR information or come and go repeatedly throughout the day may only issued this paper pass instead of an ITAR badge.



> ***Note:*** *Non-U.S. person visitors will not be allowed access to ITT facilities beyond the visitor lobby unless specific coordination is completed with Trade Compliance.*

Visitors that are not able to verify their U.S. person status will be issued one of the following types of badges. Personnel wearing the badges below must be escorted at all times.

V Escort Required

This badge is used for visitors to one of our Secure Areas but do not have the appropriate security clearance/access.

International Visitor Escort Required

This badge is used for visitors who are not U.S. persons.

Lost Badges

Lost badges should be reported immediately to the ITT SSD Security Control Center at (585) 269-6969 so that they may be deactivated.

Visitor Control

The need to protect classified (as well as proprietary information) and to protect SSD from non-employees possibly getting injured on ITT property **requires** visitors to be under escort at all times when on company premises. This is your responsibility as their SSD point of contact (POC) or host. This is a corporate policy for all visitors to SSD, whether they have accesses or not. A good rule of thumb…if an individual does not have a permanently issued SSD badge, they are a visitor and must be escorted.

Notification and Approval of Classified Visits

All classified visits require advance notification. If you are hosting visitors to any SSD secure area, it is necessary that you notify and coordinate this visit with the SSD Security office. The SSD Security Visit Control specialist must receive written notification so that they can make the necessary arrangements for the visitors to have access to the facility. Advance notification also allows security to contact the visitor's security office prior to their arrival if we have not received certification of their accesses, minimizing the chance that they will be held up at the front door upon their arrival. Your cooperation and coordination is required to ensure visits run smoothly.

Classified Visit and Meeting Requirements

All persons in attendance at classified meetings occurring in a SCIF/secure area must possess the required security clearance/access approval and need-to-know for the information to be disclosed. Need-to-know will be determined by the individual responsible for hosting the meeting. The clearance/access level of the meeting must be announced at the beginning of the meeting.

Visits to SCIFs/Secure Areas by Uncleared Personnel

Allowing access to our SCIFS/secure areas by uncleared visitors is not encouraged. All consideration must be applied to hosting uncleared visitors outside of secure areas. Requests for an exception to this policy will be considered by SSD Security on a case-by-case basis only when it is absolutely necessary for an uncleared individual to attend a meeting or perform a specific task. Exception requests should be coordinated with SSD Security as far in advance as possible so that we can determine whether holding the meeting inside a SCIF/secure area is feasible and, if so, what security precautions must be taken.

If an exception to policy is approved, a notification will be sent out beforehand and signs will be posted accordingly in order to allow employees time to sanitize (i.e. remove stray classified material from view) affected areas.

Search and Random Inspection Policy

All SSD employees, associates, and visitors are advised that in accordance with Department of Defense Regulation 5220.22-M and chapter 5, paragraph 103a of the National Industrial Security Program Operating Manual (NISPOM), all personnel and their belongings are subject to search upon either entering or departing SSD facilities. This includes briefcases, purses, packages, boxes, etc. Refusal to allow authorized employees to conduct these searches may be grounds to deny entry or to be detained for further disposition.

Further, ITT employees should be advised that all offices, desks, files, and lockers, etc. are the property of ITT. Employees should have no expectation of privacy in offices, desks or lockers, which are subject to search at any time.

Portable Electronic Devices (PEDs)

Portable Electronic Devices (also sometimes referred to as Personal Electronic Devices or Prohibited Electronic Devices) can be a serious threat to security. Therefore, only certain types or models of various PEDs are authorized for use in our secure areas. CML policy series 1600-05 contains more detailed information on which devices are prohibited and which are authorized. Unless otherwise indicated, any authorized PEDs must be registered with security and will be audited at least annually. A general list of prohibited and authorized PEDs is provided on the following pages. PED lockers (shown here) have been installed at various SCIF/Secure Area entrances for you to store any prohibited devices before entering. Questions about devices not covered by the policy should be directed to SSD Security. *Any violations of the PED policy must be reported to SSD Security!*

Prohibited Devices Inside Secure Areas/SCIFs

For various security reasons you are prohibited from bringing certain electronic devices into secure area and SCIFs. Examples of the more common types of prohibited PEDs are:

Cell Phones

Although not permitted inside SCIFs or secure areas, they are permitted in non-SCIF areas by employees without restriction. Non-ITT employees may bring their cellular phones into ITT areas subsequent to signing the PED Visitor Briefing Form (ROC-1600-20-001-01).

Recording Devices

Audio and video recording devices (whether company-owned or personal use) are **NOT** permitted inside secure areas/SCIFs. Any pictures that need to be taken inside secure areas/SCIFs must be approved by the government customer and coordinated through the security officer in accordance with ROC-1600-01-006.

Transmitting Devices

2-way

As a rule, any device with a wireless capability (i.e. it transmits or receives any type of outside signal) is usually prohibited. Examples include 2-way pagers, satellite radios, Bluetooth devices, and certain models of MP3 players such as the Zune (all models) the iPod Touch.

Personal Digital Assistants (PDA)

Almost all PDAs (to include company-provided Blackberrys) are prohibited from entering secure areas/SCIFs. There are, however, a few models of PDAs that can be modified slightly in order to be allowed. If you intend to purchase a PDA for the purpose of bringing it inside a secure area/SCIF, be sure to ask Security before you buy! Link cables and cradles are prohibited even for a PDA that has been authorized.

Media Storage Devices

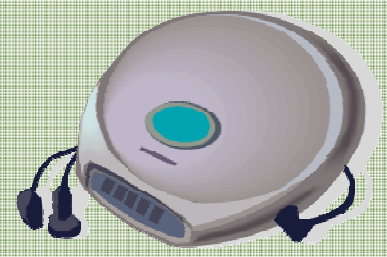
All kinds of media storage devices are either prohibited from entering our secure areas/SCIFs or cannot be removed without special authorization from Computer Security. Examples include floppy disks, memory sticks/thumb drives, and writeable CDs and DVDs (with the exception of home-burned music CDs) and the 1st generation iPod Shuffle.

Authorized Devices Inside Secure Areas/SCIFs

There are also some electronic devices which do not pose a threat to security which you may bring into SSD secure areas & SCIFs. Some examples of these authorized items are:

Music Players

Stand-alone CD players and MP3 Players that cannot record and do not have wireless transmission capability or a male USB port may be brought into secure areas/SCIFs and do not need to be registered with Security. Remember though that the docking cables and cradles are not allowed.



Music CDs

Store bought and home-burned music CDs may be brought into secure areas/SCIFs; however, home-burned CDs must be labeled as such and have your name on it. Music CDs can only be played on stand-alone CD players and must never be played on any company-owned computer.

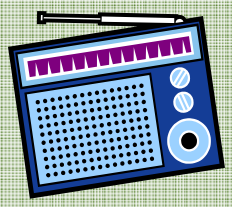
Pagers (1 or 1½-way)

Pagers that receive only or can transmit only canned messages are permitted inside the secure areas/SCIFs.

1-1½ -way

Radios

Simple AM/FM radios with no recording capability are authorized to be brought into secure areas/SCIFs and do not need to be registered with Security.



Information Security

The primary function of SSD Security is the protection of U.S. government national security information that has been deemed classified in the interests of national security. We also provide assistance in the protection of U.S. export controlled information and company proprietary information. The purpose of your obtaining a security clearance is to be able to handle this sensitive information and material in order to do the job for which you have been hired in support of U.S. government contracts we have won. The following section will define classified information and its various levels of sensitivity as well as some key terms you need to know in the handling and protection of classified information. This section will also explain why information is classified, how it is classified, how to identify and mark it, and how to handle and safeguard it.

Executive Order (EO) 13292 Further Amendment to EO 12958, As Amended, Classified National Security Information

E.O. 13292 and 12958 prescribe a uniform system for managing the protection of national security information. They describe two classification processes: *original classification* and *derivative classification*. The new standard set forth in the Orders is that information will normally be classified for only 10 years. If it is necessary to extend classification beyond 10 years, specific action is required to obtain an extension or an exemption from the rule.

The E.O. 13292 and 12958 increase personal accountability for the management of classification. The Orders also detail proper procedures for marking and safeguarding classified information and establish new processes for classification challenges, self-inspection programs, and oversight of special access programs. Finally, the Orders add classification management as a critical element for evaluation during performance reviews for employees who handle and create classified information.

Contractor Program Security Officer (CPSO)

The Director of Security, Robert Washburn, is the *CPSO* for ITT Space Systems. He is responsible for implementing all program security policies relative to classified activities within SSD and ensuring full compliance with all applicable security manuals, requirements, and directives.

Definition and Levels of Classified Information

Classified Information is information which the United States government has determined to be vital to the national defense of our country. Information is classified pursuant to Presidential Executive Orders (E.O.) 12958 and 13292. Classified information is designated and marked as either *TOP SECRET, SECRET* or *CONFIDENTIAL* based on the level of damage it would cause to national security if it were compromised (disclosed to unauthorized persons) as described below:

TOP SECRET – would cause exceptionally grave damage if compromised;

SECRET – would cause serious damage to national security if compromised; and

CONFIDENTIAL - would cause identifiable damage if compromised.

UNCLASSIFIED - marking used to specifically identify information that has been specifically reviewed and certified to not contain classified information.

FOR OFFICIAL USE ONLY (FOUO) - FOUO is not a classification but rather a handling caveat sometimes used to identify UNCLASSIFIED information that must be afforded special handling because it **should not be released** to the general public. Information that meets this description is marked at the top and bottom center of a page:

UNCLASSIFIED//FOR OFFICIAL USE ONLY

The following rules apply to the handling for FOUO information:

- FOUO may only be taken out of a secure area for official business only
- FOUO must be kept locked up when not in use, and
- FOUO must be returned to the secure area for destruction. It must be put into a burn container for destruction.
- FOUO can only be sent via email by a government entity; contractors must not send or forward FOUO information by email.

> ***NOTE:*** *The President of the United States announced in May 2008 that the new designation CONTROLLED UNCLASSIFIED INFORMATION (CUI) has been approved and will eventually replace UNCLASSIFIED FOUO and a myriad of similar designations such as SENSITIVE BUT UNCLASSIFIED (SBU) which are currently in use.*

Basic Rules Regarding Classified Information

Need-to-Know

Need-to-know is the fundamental principle in the protection of classified information. It is a determination by an authorized holder of classified information that access to information is required by another appropriately cleared individual to perform official duties.

YOU, as an authorized holder, have the authority and are empowered to grant or deny access to any other appropriately cleared individual. It is your responsibility to confirm in your mind that he/she truly needs the information to do his/her job. The individual in question must be able to give you sufficient justification so that you can make an informed *need-to-know* decision.

Need-to-know is one of the most difficult security principles to apply. It violates our inherent social nature and promotes a level of personal responsibility that most of us find difficult to accept. However, failure to accept this responsibility has resulted in some of the most damaging espionage cases in the last decade. Statistically, the FBI reports that "insiders" commit 80% of espionage. Most of these "insiders" who committed espionage were fully cleared individuals, some with access to special program information. In almost every case, these "insiders" gained access to information not pertinent to their jobs by circumventing the *need-to-know* principle. They were able to do so because their co-workers failed to properly control access to classified and restricted information under their control.

Applying Need-to-Know

When sharing classified information with co-workers, you must be sure that they have not only the appropriate clearances and access levels, but also a clear "need-to-know" the information. Establishing need-to-know is important in controlling classified material. To make this determination, whoever holds classified material should ask the following questions before sharing the information:

- Is the person appropriately cleared and briefed for access to this information?
- Why does the other person need the information?
- Is the information requested pertinent to the person's task/project?

After considering the questions above you have three choices of action:

1) **Grant access**—you are certain the individual is authorized access to the level of the material and it is needed by them in the performance of their job;
2) **Deny access**—you are certain the individual is either not cleared for access to the level of the material or they do not need access to it in the performance of their job; and
3) **Delay access**—you are uncertain as to whether the individual is cleared for access to the level of the material or cannot confirm that they need access in the performance of their job and wish to consult with Security, your supervisor or some other knowledgeable individual before making another determination.

Dual Responsibility. Responsibility also applies to individuals who are requesting information. If you do not have a "need-to-know" you should not be inquiring into the information. This is particularly applicable to individuals who have left programs to work in other areas or on different projects.

Classifying Information: Original vs. Derivative Classification

There are two methods used to classify information: original and derivative. An original classification decision for any level of classification can be made only by an Original Classified Authority (OCA) which is a U.S. government official who has been delegated the authority in writing by the President of the United States. We, as contractors, make *derivative classification* decisions only.

Derivative classification means that you incorporate, paraphrase, restate, or generate in new form, information that is already classified. As a derivative classifier, you refer to either a classified source document or a classification guide and mark newly developed materials consistent with the source markings or the instructions in the guide.

In doing derivative classification, you will need to understand the levels of classification, what is and isn't classified, the duration of classification, and document marking.

There are two common scenarios you will encounter in doing derivative classification:

1) Sometimes you will be copying, restating or paraphrasing information from a single classified document as you prepare your new document. In this case, you will put markings on your new document consistent with those found on the source document. If you use classified information from more than one source document, ensure you mark your new document with the highest classification of any of the information you have used. If you have any doubt about the proper classification to use, check the security classification guide covering the subject. A complete list of all the sources used must be attached to the end of the official file or record copy of the classified document.

2) In another situation, you will be creating a document without taking information from source documents. Here, you'll check the appropriate classification guide for proper classification instructions.

If, after reviewing classification guidance, you have **significant** doubt regarding the classification of a specific piece of information, **DO NOT** classify it. If you are unsure, consult the SSD Security Office; who may, in turn, need to contact one of our U.S. government customers.

Information may **not** be classified for the purposes of:

- Concealing violations of law, inefficiency, or administrative error;
- Preventing embarrassment to a person, organization, or agency;
- Restraining competition; or
- Preventing or delaying the release of information that does not require protection in the interest of national security.

Basic scientific research information not clearly related to national security may NOT be classified. Information may NOT be classified after it has been declassified and officially released to the public.

Co-Use Agreement

Each of our SCIFs are sponsored by a particular government customer/agency. The policy of this agency is to prohibit classified material from another customer/agency into their sponsored SCIFs unless there is a co-use agreement in place with the other customer/agency. A list of current existing co-use agreements is available in the SSD Security Office for review.

Downgrading or Declassifying Classified Information

Information is downgraded or declassified based on the loss of sensitivity of the information due to the passage of time (no longer state-of-the-art) or on occurrence of a specific event. SSD will downgrade or declassify information based on the guidance provided in a Contract Security Classification Specification (DD254, NF 4.4702), upon formal notification, or as shown on the material. These actions constitute implementation of a directed action rather than an exercise of the authority for deciding the change or cancellation of the classification. At the time the material is actually downgraded or declassified, the action to update records and change the classification markings will be initiated and performed unless directed otherwise. Declassification is **NOT** automatically an approval for public disclosure.

Classified Information Appearing in Public Media

The fact that classified information has been made public does **NOT** mean that it is okay to talk about it. When classified programs are declassified, the government does not always declassify each or every portion of a program—do not assume. You must continue to protect the information until you have been formally advised to the contrary. Questions as to classification in these cases should be brought to the immediate attention of SSD Program Security who will, in turn, contact the appropriate government customer.

Classified Material Marking Requirements

As a general rule, **ALL** classified information, regardless of the form in which it appears, requires marking. Marking some equipment/material is difficult, but since the principal purpose of the marking is to alert the holder that the information requires special protection, it is essential that all classified material be marked to the fullest extent possible.

Classified material is required to be marked with all of the following that apply:

- Overall classification level (Top Secret, Secret or Confidential)
- SCI Control System(s)
- Dissemination controls and/or special handling caveats
- Document control and accountability number
- Date of the material
- EO 12958 Classification Block (to include the E.O. eligibility for expiration code)
- Portion Markings

Note: *SSD Security has developed a local classified information marking course for cleared employees which is available on the Security Education and Awareness page of the classified Security web portal. For more information please refer to course SEC-00011 on the TEMS database on the unclassified SSD portal. Classroom sessions are also available upon request.*

Executive Order 12958 Classification Block

EO 12958 went into effect in 1995 (amended 2003) and added this additional marking to all classified government information. It indicates the eligibility for declassification date. This is a government-wide marking. The classification block marking must appear in the lower left corner of the document's front page.

The classification block originally contained four items Classified By (CL BY), Classification Reason (CL REASON), Declassify On (DECL ON), and Derived From (DRV FROM). This four-line block has since been replaced by a two-line block for derivative classification decisions, which are what we perform, containing only DECL ON and DRV FROM.

As a general rule, a "Classified By" line and a "Reason Classified" line will be shown only on originally classified documents. Certain agencies may continue to require these additional two lines – Classified By and Reason Classified. If this is the case, instructions will be included in the security classification guidance provided with the contract. The various Reason Classified exemption categories are as follows:

(X1) reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;

(X2) reveal information that would assist in the development or use of weapons of mass destruction;

(X3) reveal information that would impair U.S. cryptologic systems or activities;

(X4) reveal information that would impair the application of state of the art technology within a U.S. weapon system;

(X5) reveal actual U.S. military war plans that remain in effect;

(X6) reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

(X7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

(X8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security;

(X9) violate a statute, treaty, or international agreement.

Two-Line Classification Block

DECL ON: Most DoD documents will show a declassification date of 10 years from the date of their creation. For all of our SCI materials, the exemption category 25X1 must be used. Exemption category X1 is defined in section 3.3 of E.O 12958 (amended) and extends a document's classification from ten to at least 25 years. The 25X1 marking is applied when information is exempt from the 25-year automatic declassification.

DRV FROM: The "Derived From" line indicates which classification guide, or whom you consulted to derivatively classify the document. On this line, you would place the title and date of the classification guide or source document. If you are using more than one source document or classification guide to assign classification markings to a new document, this line would read "Multiple Sources" and a complete list of all the sources used must be attached to the end of the official file or record copy.

Example 1: DECL ON: 25X1, YYYYMMDD, {govt. agency reference if applicable}
DRV FROM: IMINT PCG 25 MAY 05

Example 2: DECL ON: 25X1, YYYYMMDD, {govt. agency reference if applicable}
DRV FROM: Multiple Sources

Portion Marking

A portion is a part of a document: a paragraph, title, chart, figure, caption, sidebar, or illustration. Each portion of a document must be marked to indicate which portions are classified and which portions are unclassified.

To indicate the appropriate classification level, place the following symbols at the beginning of each portion:

- (TS) for TOP SECRET
- (S) for SECRET
- (C) for CONFIDENTIAL, (DOD Only)
- (U) for UNCLASSIFIED
- (FOUO) For Official Use Only

If the portion contains SCI information, you must use the SCI digraph/trigraph separated by a slash after the classification.

For example: (TS//TK) or (S//TK)

Document Control and Copy Number

Document Control and Copy Numbers are required if the material is "formally" accountable. A Document Control Number is required on any material that is being transmitted outside SSD (for tracking purposes). For formally accountable material, the Document Control and Copy Number must appear in the upper right hand corner of **each page** of the document. For all other material transmitted outside our company, the Document Control Number needs to only appear on the cover sheet.

If you are planning on transmitting material outside SSD, obtain the appropriate Document Control Number from your SSD Security Office. Be prepared to communicate the classification level and compartmentation, if applicable, to the security personnel.

Marking Transmittal Documents

An unclassified memo or document that transmits a classified document as an attachment must bear the most restrictive classification of the attachments it is forwarding as well as the following handling notation:

UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ATTACHMENTS

Marking Compilations

In some instances, information that is unclassified when standing alone may become classified when combined or associated with other unclassified information. When classification is required to protect a compilation of such information, the overall classification assigned to the document must be marked at the top and bottom center of each page and on the outside of the front cover. The reason for classifying the compilation must be stated at an appropriate location at or near the beginning of the document. In this instance, the portions need not be marked.

Marking Working Papers/Notes

Classified working papers generated in the preparation of a finished document shall be: (1) dated when created, (2) marked with its overall classification and with the annotation “WORKING PAPERS”, and (3) destroyed when no longer needed.

Contractor Developed Information

Whenever we develop unsolicited proposals or originate information not in the performance of a classified contract, the following rules apply:

a. If the information was previously identified as classified, it will be classified in accordance with an appropriate Contract Security Classification Specification (DD254), classification guide, or source document and marked as required.

b. If the information was not previously classified, but we believe the information may, or should, be classified, we should protect the information as though classified at the appropriate level and submit it to the agency that has an interest in the subject matter for a classification determination. Submission should be made via SSD Security. In this case, the material should be marked according to what you believe the classification should be preceded by the word “TENTATIVE”:

TENTATIVE _____ (TOP SECRET, SECRET, or CONFIDENTIAL)

This marking will appear conspicuously at least once on the material but no further markings are necessary until a classification determination is received. In addition, we are not precluded from marking such material as company proprietary information. Pending a final classification determination, we should protect the information. It should be noted however, that E.O. 12958 & E.O. 13292 prohibit classification of information

over which the Government has no jurisdiction. To be eligible for classification, the information must:

1) Incorporate classified information to which we were given prior access, or

2) The Government must first acquire a proprietary interest in the information.

Marking Downgraded or Declassified Material

There is no requirement to remark downgraded, decompartmented, or declassified materials unless they are being transmitted outside our facility. If being transmitted, they should be re-marked as follows:

1. **Automatic Downgrading, Decompartmentation, or Declassification Actions**

   As a minimum, the outside of the front cover (if any), the title page (if any) and the first page must reflect the new classification markings, or the designation UNCLASSIFIED. Other material must be re-marked by the most practical method for the type of material involved to ensure it is clear to the holder what level of classification is assigned to the material. Old markings must be canceled, if possible. If not practical, affixing new decals, tags, stickers, and the like to the material or its container may mark the material.

2. **Other than Automatic Downgrading, Decompartmentation, or Declassification Actions**

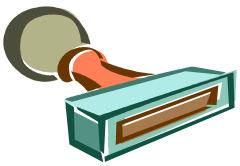
   When notified, all old classification markings must be canceled and new markings substituted, whenever practical. As a minimum, the outside of the front cover (if any), the title page (if any) and the first page must reflect the new classification markings or the designation UNCLASSIFIED. In addition, the material must be marked to indicate the authority for the action, the date of the action, and the identity of the person or contractor taking the action.

Marking Wholly Unclassified Material

Marking wholly unclassified material is not required unless it is essential to convey to a recipient that the material:

1) has been examined specifically with a view to impose a security classification and has been determined not to require classification; or

2) has been reviewed and has been determined to no longer require classification and has been declassified.



Information Security

Safeguarding Classified Information

The following sections describe the proper safeguarding and handling regulations which apply here at SSD:

Open Storage

Several SSD SCIFs/secure areas have been approved by our government customer for "open storage." An open storage policy applies to U.S. government classified material and means that you may leave classified material on your desk when you leave at the end of the day or you may store classified material in a safe, file cabinet, desk, etc. that does not need to be locked.

> ***Note:*** *This Open Storage approval applies to U. S. Government classified material; it* ***DOES NOT*** *apply to SSD Proprietary information.*

We have been granted approval and authorized for this due to in-place physical security measures and our GuardsMark security force which will respond 24 hours a day, seven days a week in less than 5 minutes to any alarm.

Although approved for open storage, you should maintain some control over your work area as we occasionally need to escort uncleared individuals into our secure areas for a variety of reasons. Before this happens, the secure area must be *sanitized* which entails removing all classified material from view. Proper upkeep of your work area ensures the job of sanitizing does not become a task that takes days … but only 5-20 minutes.

> ***Note:*** *If you leave classified information laying around within the secure area and someone walks by your desk and it is taken (or borrowed), there is no way SSD Security is going to be able to help you determine where that material went. Being in an approved secure area with Open Storage does not relieve us of our responsibility to maintain positive control over classified information.*

Open storage is approved for all SSD SCIF locations at Hawkeye, RTP-6, and Bldg. 101.

Open storage is not approved for:

- The VOIT and VINCENT DoD labs at Hawkeye;
- The Washington (Herndon, VA) office;
- The Bloomfield, NJ facility
- EM program material;
- SY program material; and
- Various other compartmented/special materials.

Classified Material Storage Equipment

For areas where open storage is not permitted, a Government Services Administration (GSA) approved classified material storage container must be used.

Safes

The most common type of GSA-approved storage container is commonly referred to as a safe.

To obtain a safe for your office in any SSD building, contact the Government Property Administrator at (585) 269-5113.

If you are the custodian of a safe which contains material that must still be locked (i.e. material that does not apply to our Open Storage accreditation) it must have a SALMON colored Container Card (FSD 2228) affixed to the front of it with the appro-

priate information. This indicates that the safe MUST BE LOCKED/SECURED at the end of each day and during non-working hours. Each such safe is on the checklist supplied to the guards ensuring they will check it each evening to ensure it is properly secured. If these safes are found open after hours by the guards, a violation will be written and the Custodian and Security will be called at home.

Changing Safe Combinations

Combinations must be changed upon compromise or suspected compromise. If you are the custodian of a safe and have material stored which must still be locked, and you feel the combination has been compromised in any way, please notify Security and we will change the combination for you.

SSD Security maintains a master combination list for all containers. If you would like your combination changed or have forgotten a combination, give the SSD Security office a call.

Cover Sheets

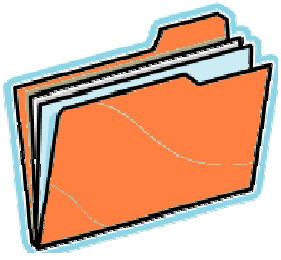
ALL classified material must have the appropriate cover sheet affixed to it. If you don't have the necessary cover sheets, they are readily available at SSD Security and on both Security web pages (unclassified and classified LAN). Using cover sheets makes classified material easily identifiable and helps in precluding it from getting mixed in with unclassified materials and inadvertently taken home, on trips, etc.

DoD Cover Sheets

SCI Cover Sheets

Orange Folders

It is an SSD highly recommended practice that all classified hardcopy information be placed in orange folders. Special attention must be given to ensuring that all SCI information is placed in orange folders when walking around within the SCIF. This makes it easily identifiable and when used in combination with the cover sheets above helps preclude classified material from getting mixed in with unclassified materials and inadvertently taken home, on trips, etc..



Control and Accountability

Unless specifically directed otherwise by contract, only Top Secret DoD information is required to be formally controlled. All other information is no longer required to be formally controlled. This means the only materials you will be required to sign for in writing will be Top Secret DoD materials. This includes documents, disks, tapes, built-in hard drives, etc. Other classified information must still be properly protected, but it will not be formally tracked EXCEPT when receiving and transmitting these materials into/outside our facility.

Inventories

Once a year, those individuals who have materials that are formally accountable will receive an inventory listing these materials. It is a contractual requirement that an annual inventory be conducted and a record created showing the date of the inventory, name of the individual(s) conducting the inventory and any discrepancies noted. Once completed, the inventory must be returned to the security office for retention. Security will follow up with you on any discrepancies noted.

Working Papers/Notes

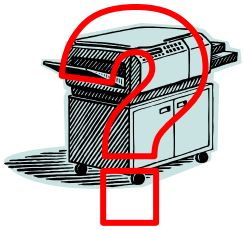
Classified working papers generated in the preparation of a finished document shall be: (1) dated when created, (2) marked with its overall classification and with the annotation "WORKING PAPERS", and (3) destroyed when no longer needed. Working papers shall be marked in the same manner prescribed for a finished document at the same classification level when: (1) transmitted outside the facility, or (2) retained for more than 30 days from creation for TOP SECRET, or 180 days from creation for SECRET and CONFIDENTIAL material.

Faxes

Normally, classified faxes are no longer formally tracked. However, if your fax contains formally accountable information, it will need a Document Control Number on it prior to transmission and its transmission will be logged in the SSD Security Document Control system database.

Reproduction

You may reproduce program material unless there is a prohibition against it written on the document. Even if there is no prohibition, the reproduction of program material should be kept to a minimum. Use only approved copiers (i.e. those within secure areas). All copies of program documents are subject to the same marking, control, accountability and destruction procedures as the original. After classified material has been reproduced, the operator is responsible for ensuring the appropriate cover pages are applied to all copies and all classified material is retrieved.



Discussions

In order to discuss classified program information, you MUST use a secure area that has been specifically accredited for the particular programs to which you have access. Be aware that lobby areas, elevators, stairwells, bathrooms, cafeterias, gyms, garages, vehicles, commercial airlines, etc. are NOT approved areas for classified discussions. If it appears that a conversation may possibly broach classified information, terminate it immediately and, if necessary, continue the discussion in an approved secure area. Contact Security for your specific location's non-discussion areas.

Transmission

Some general information on the methods and procedures for transmitting classified information/material outside of SSD is provided below. Specific detailed information on this policy, procedures, and the forms for transmitting classified information/material is located in CML Document series ROC-1600-20-007.

As a general rule, **all hard copy classified materials are received and dispatched by SSD Security**. It is required that transmittal receipts accompany all classified transmittals. Receipts for outgoing materials will be generated and tracked by SSD Security. Receipts accompanying incoming transmittals will be verified, signed and returned to the originating agency in a timely manner by SSD Security Office personnel.

DoD Classified Information (Secret and below)

DoD (Collateral) information that is classified at the SECRET and below level may be sent via the U.S Postal Service or another government authorized courier (e.g. Federal Express, UPS, DHL, etc.). If someone is sending you material of this type, the address you should provide them to ship it to is as follows depending upon your work location:

Rochester:

USPS - United States Postal Service overnight (preferred method of shipment)
ITT Space Systems, LLC
Attn: Facility Security Officer
PO Box 17259
Rochester, NY 14617-7259

This material is delivered to our PO Box and then picked up by a courier on the Product Transportation team, then delivered to the Security office 3-11-HE. The Facility Security Officer (Mary Ann Optis) is then called for pick-up.

For FedEx, UPS, or other approved courier shipments (FedEx preferred):
ITT Space Systems, LLC
Attn: Facility Security Officer
1447 St. Paul Street
Rochester, NY 14621

This material is shipped to the above address and is received on our dock by shipping/receiving (Bob Sutherland) and then he calls the FSO for pick up.

Bloomfield:

USPS - United States Postal Service overnight (preferred method of shipment)
ITT Space Systems, LLC
Attn: Facility Security Officer
PO Box 1062
Bloomfield, NJ 07003

For FedEx, UPS, or other approved courier shipments (FedEx preferred):
ITT Space Systems, LLC
Attn: Facility Security Officer
1515 Broad Street, Bldg. D
Bloomfield, NJ 07003

DoD Top Secret and SCI Information

DoD TOP SECRET and SCI level information must be sent either via an official government customer courier (or via individual hand-carry). The current courier schedule for outgoing SCI material is every other Tuesday only for Rochester (every Monday only for Merrifield). If you have courier material to go out, it must be brought into Security at least three days prior to the next scheduled courier day to allow Security time to process the receipts and prepare the materials for shipment.

Individual Hand-carries

In urgent cases where other options are not available, SSD employees may hand carry classified material to another location or facility. Before being authorized, individuals must first receive a Courier Briefing and be issued a Courier Authorization Letter by SSD Security. SSD Security will also wrap the material to be hand carried and generate a transmittal receipt.

Secure E-mail

Classified information may be transmitted outside of SSD via secure email.

- SCI – SCI information can be sent via either CWAN (Contractor Wide Area Network) or GWAN (Government Wide Area Network).
- Collateral (DoD) – DoD information at the SECRET level only can be sent via SIPRNET.

Secure Fax

We can send classified documents via a Secure Fax in most instances (depending upon which government agency sponsors the facility in which the material needs to be sent). A properly completed Fax Cover Sheet (ROC-1600-19-001-01) must accompany all outgoing faxes. The Fax Cover Sheet becomes page one of the document you are faxing, therefore all markings that apply to your document, will apply to your fax cover sheet. Material to be faxed should be marked the same as any other material.

- Outgoing Faxes - All Rochester Security offices have an In-Box for your outgoing faxes. Place all of your routine faxes into this in-box. As a general rule, routine faxes will be transmitted either immediately or within 30 minutes of being placed in the in-box. If you have a Priority fax, when placing it into the in-box, please let someone in the Security office know that your fax needs to go out immediately. Once faxes are sent, they are marked with the date and time of transmission and placed into the appropriate mail folder or otherwise held for the owner. **Washington** personnel must contact the Facility Security Officer for assistance.
- Incoming Faxes - When the office receives an incoming fax for an individual, the addressed individual will be notified by phone and the fax will be placed in the appropriate mail folder or otherwise held for the addressee.
- DoD Material Faxes - All incoming and outgoing DoD faxes will be processed by the Facility Security Officer (FSO).

Telephones

Other than your commercial company line, there are three other types of telephones you may encounter within SSD:

1) **Sterile Telephone Unlisted Meter Business Lines (UMB) (Hawkeye only)**

   This is sometimes referred to as a "Hello" phone. This is because when you answer it, you answer it by saying "Hello." This phone is leased under an individual's name and as far as anyone knows, it does not belong to a place of business. Therefore, you should never mention the company's name or geographic location on these phones. These phones are for UNCLASSIFIED conversation only.

2) **STU-III; Secure Telephone Unit, version three.**

   STU-IIIs operate as normal telephones until you insert and turn a key and press a Secure Voice button. The phone is then electronically configured to scramble your conversation. When calling on the STU, the first thing you need to do is to make sure to whom you are speaking. This is done by voice recognition. Once you have the right person on the other end, simply tell them you are initiating secure voice mode by pushing the button. Once the LED adjacent to the Secure Voice button lights up, you may talk CLASSIFIED up to the level indicated by the LED screen which displays the level of the other party's approved access. The digital readout will let you know which mode the phone is in at all times.

3) **Secure Phones (RED phones)**

   This phone is for classified discussions. You may assume the person you are talking with at the other end is briefed. You must still know who you are talking with regarding any specific compartments and use basic "need to know." The secure phones located in the Merrifield office are not actually red but are identified by a large yellow and black label.

Document Disposition & Retention

SSD documents (including classified documents) should be disposed of or retained in accordance with SSD-0400-01-004 and/or individual contract requirements.

Disposition / Destruction

All white paper in our SCIFs must be disposed of in the red burn receptacle bins located throughout SSD secure areas. Formally accountable documents, however, must be brought to SSD Security for disposition for tracking purposes.

All magnetic media containing classified or unclassified information must be disposed of in designated receptacles located within each secure area. Security can direct you to the receptacle locations.

> ***Note:*** *In the Washington Office, see the Facility Security Officer for disposition of classified material.*

Outside of secure areas and SCIFs all white paper waste should be deposited in a gray bin shown on the right which is approved for ITT proprietary and ITAR information waste.

Retention

Per Government directive, we may retain classified material received or generated under contract for a period of two (2) years beyond receipt of final payment and contract close out. Retention beyond this period requires a written request to and approval from the appropriate Government Contracts office.

Equipment & Material Removal

If you have items leaving an SSD facility, follow material removal procedures specified in CML document ROC-1600-20-005 (Material Removal). All cabinet and container removals from secure areas require additional scrutiny and adherence to specified procedures cited in CML document ROC-1600-20-008 (*Furniture and Container Removal from Secure Areas)*. Additionally, random inspections by our uniformed security guards are conducted at the entrances/exits of secure areas. These inspections include briefcases, folders, boxes, etc.

Emergency Procedures

Each facility has an established emergency evacuation procedure/route. It is your responsibility to contact the Emergency Coordinator in your facility to determine your responsibilities when evacuating the facility. If you don't know your Emergency Coordinator, stop in and we'll get the information for you. During an emergency, remember that your personal safety is our primary concern. Do not jeopardize your well-being in order to protect classified material. Regardless, when it is necessary to evacuate the facility, keep the following in mind:

- If it is possible to do so without endangering yourself, close and lock any security containers you may pass as you exit the building.
- If you have a STU-III phone in your office, pull out and lock up the crypto-ignition key (CIK) or just put it in your pocket and walk out with it.
- DO NOT TAKE ANY CLASSIFIED INFORMATION FROM THE FACILITY UNLESS IT IS ABSOLUTELY UNAVOIDABLE. If you find yourself in this situation, conceal the information as best you can and immediately come into the SSD Security Office to report the incident at the first opportunity after the occurrence.

Personal Cover Stories

A common question many people have after getting cleared is, "What should I say when people outside of work ask me about my job?" Outside work, it is prudent to say as little as possible about your job so as not to arouse undue interest. Your security officer can assist you in anticipating answers to questions you might be asked in a social setting. For instance:

- When asked about your job, give a generic statement (e.g., research engineer, technical analyst)
- When asked about what your company does, reply with a general description (e.g., defense technical services, or support and analysis)
- When asked about a specific classified program in which you are engaged, say that you are not at liberty to discuss the details of your work.

Information Security

Information Systems (Computer) Security

Information Systems (Computer) Security is the security discipline which enforces customer and corporate policies regarding the use of automated information systems in the protection of proprietary company information and U.S. government classified national security information on information systems within a secure environment. The types of electronic equipment governed include but are not limited to:

- Classified Computers
- Unclassified Computers
- Portable Electronic Devices (PEDs) (e.g. PDA's, Jump Drives, USB Devices, etc.)
- Cellular Telephones

Information Systems Security Manager (ISSM)

The ISSM is the SSD Security individual with specific overall responsibility for AIS Security services.

Information Systems Security Officer (ISSO)

SSD Security has assigned an ISSO to each facility with secure areas. ISSOs are specifically responsible for providing AIS security support services at their facility.

Computer Security Policies and Guidance

SSD Computer Security rules, regulations and policies are based on and in compliance with directives from higher authority to include:

- Corporate Policy: Information Security Policy 70-02 — applies to unclassified computers and networks.
- Government Intelligence Community Customers & Contracts: Director Central Intelligence Directive (DCID 6/3) — applies to classified computers and networks.
- Department of Defense (DoD) Customer Contracts: National Industrial Security Program Operating Manual (NISPOM) – Chapter 8 (NISPOM Chapter 8) — applies to DoD labs.
- Individual Contract Classification Guides & System Security Plans

ISNET (Imaging Systems Network)

ISNET is a classified computer network owned by our primary sponsoring government agency.

Account Access

In order to obtain permission to access and establish an account for ISNET an individual must be properly briefed and issued an SSD badge with a full black stripe. Information on requesting an ISNET account is contained in CML documents SSD-0900-03-019 and SSD-0900-03-019-05.

Joint-Use Agreements

It is essential for you to know who the customer is relative to the contract you are working on. Other agencies contract work cannot be conducted on ISNET unless a joint-use agreement exists between the owning agency and your other customer. A current joint-use agreement list is available in the SSD Security Office for review.

Equipment Labeling

Classified information may be processed only on approved automated information systems (AIS). A computer system approved for classified processing will be labeled with a YELLOW/BLACK sticker that reads "AUTHORIZED FOR CLASSIFIED USE" (shown below).

AUTHORIZED FOR CLASSIFIED USE

Terminals designated for unclassified use will have a GREEN/BLACK sticker which reads "UNCLASSIFIED USE ONLY" (shown below). Unclassified computers/terminals are **NOT** to be used for classified information.

UNCLASSIFIED USE ONLY

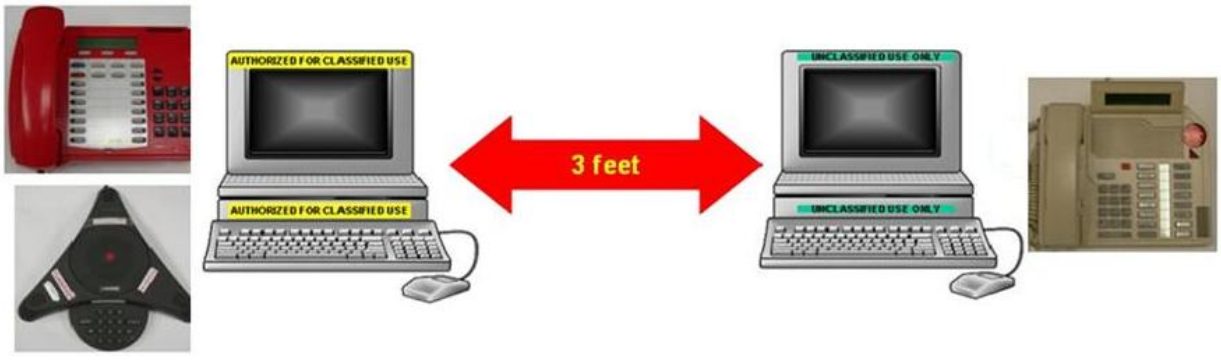
Contact SSD Computer Security if you discover any equipment that is not labeled.

Media Labeling

All media MUST be labeled. This includes vendor media, read only media, media found in the back of a text book, etc. It must be classified and labeled to the highest level of information that has ever been written to the media (i.e. Top Secret, Secret, SI, TK, etc). Labels for floppy disks are available in the Security Office. CDs/DVDs must be labeled with a permanent marker with the labeling applied to the media itself, not the case. Per SSD policy (ROC-1600-01-003), no media (except home burned or commercially produced music media) can leave any of our secure areas without an approved Media Sanitization and Release Form (ROC-1600-01-003-01).

Red/Black Separation Rule (aka Three Foot Separation Rule)

It is a government requirement that classified (or **Red**) information processing and communication equipment maintain at least three feet of separation from unclassified (or **Black**) equipment. This includes phones, CPUs, monitors, keyboards, printers, scanners, etc..
Where possible, SSD Security recommends that Red and Black equipment not be co-located on the same table or desk.



Software Requests on ISNET

The use of any foreign software or hardware on ISNET is strictly prohibited! Specific authorization is required from Security and IT prior to the purchase and installation of software for use on ISNET. For additional information refer to the SSD-1600-01-002 document series in the Command Media Library.

File Transfers

Unclassified Network to ISNET

The transfer of files/data from the unclassified network to ISNET is authorized and can be accomplished by following the procedure *Data Transfer from Unclassified network to ISNET* (ROC-1600-01-001) found in the Command Media Library.

ISNET to Unclassified Network

Release of data from ISNET is risky and highly discouraged! You are required to create unclassified data on the unclassified network. As a general rule, file transfers from ISNET to an unclassified system will not be practiced except in unique cases. The procedure *Removing Data from ISNET* (ROC-1600-01-003) found in the Command Media Library explains how to do this.

Overnight Logons on ISNET

To remain logged on overnight or when away from the facility, the user must acquire prior authorization from the ISSO/ISSM. To obtain authorization send an email to SSD-Overnight@itt.npa.gov. State in detail why you need authorization, the workstation name and the location of the workstation. For more information concerning this policy please read Command Media Library SSD-1600-01-004.

Photography in Secure Areas

The use of any personal image capturing equipment in SSD secure areas is strictly prohibited! Official photography using company-owned equipment is regulated and coordinated through SSD Computer Security and described in CML policy ROC-1600-01-006.

Data Spills

Contaminations or data spills occur when classified data is released on an unclassified PC, network, or voice mail. If you suspect such an incident may have occurred—***do not touch or delete anything!*** Notify the ISSM or your facility's ISSO in Computer Security as soon as possible. The ISSM or ISSO will perform a preliminary investigation of the incident to verify the occurrence, determine extent, and identify corrective actions in conjunction with IT personnel and our government customers.

All personnel must pay particular attention to proper utilization of both ISNET and the unclassified network. Failure to do so may result in data spills that can have dire consequences. These include: irreparable damage to National Security, costs of thousands of dollars to Space Systems Division, damage to SSD's reputation, disruption of work productivity and loss of man-hours. Data spills always result in the completion of Security Violation reports and sometimes Performance Counseling and could result in termination!

Portable Electronic Device (PED) Mitigation Table

The table below depicts which PED capabilities and functionalities are prohibited from entering SSD Secure Areas and SCIFs and which are permitted and if so what, if any, mitigation is required.

PED Functionalities	Introduction & Use Permitted?	Exceptions & Footnotes	Mitigation Required Prior to Use	Approval & Registration Required?
Single–Function RF Receiver (e.g. AM/FM Radio, 1 or 1 ½- way Pager, etc.)	Yes	May not have external cabling or contain any internal or external connectivity capabilities.	None	No
CD Player	Yes	None	None	No
CDs (commercially-produced)	Yes	None	None	No
CDs (home-burned)	Yes	Must be labeled as "Music CD, Personal Property of (employee's first and last name)"		No
MP3 Players with no transmitting capability or built-in male USB connectors (e.g. IPODs)	Yes	None	None	No
Medical Devices (e.g. hearing aids, amplified telephones handsets, heart pacemakers, etc.)	Yes	Allowed IAW the customer's Reasonable Accommodation policy		No
Audio recording capability (*i.e. has a microphone port)	Generally Prohibited	May be approvable by SSD Security with prior mitigation	Disable wiring or use Adapter/ Erase Plug (see note 2)	Yes
Infrared (IR) capability	Generally Prohibited	May be approvable by SSD Security with prior mitigation	Metal Tape over IR port (see note 1)	Yes
Privately owned PEDs capable of connecting to systems within the SCIF without interface cables or cradles	Generally Prohibited	May be approvable by SSD Security with prior mitigation	Metal Tape over IR port (see note 1)	Yes
Photographic or video recording capability	No	Always prohibited – no mitigation possible		
Cellular Phones	No	Always prohibited – no mitigation possible		
RF Transmitter (e.g. 2-way pager)	No	Always prohibited – no mitigation possible		
Wireless Transmitting Capabilities	No	Always prohibited – no mitigation possible		
Privately Owned Laptops	No	Always prohibited – no mitigation possible		
Removable storage media for privately owned PDAs and PEDs (e.g. memory sticks, thumb drives, flash memory, etc..)	No	Always prohibited – no mitigation possible		
Cables & cradles for privately-owned PEDs	No	Always prohibited – no mitigation possible		

Footnotes:

1 Metal tape must be applied to the IR port by SSD Security office.

2 Microphone wires must be cut/disabled on non-laptop PEDs. An adapter/erase plug must be inserted into the laptop external microphone port(s). Any adaptor that is designed for the external microphone port may be used provided that the adapter does not provide any functionality other than disabling the internal microphone.

Index

Index

Security Depends On YOU!