STANDARD OPERATING PROCEDURES (SOP) FOR ITT CLIFTON FACILITY

ITT

01 February 2011

COORDINATED BY:

Thomas A Oceanak / CPSO

APPROVED BY:

Vernon Utley, IA-4 GSSO
Chief, Acquisition Security Branch

ADDITIONAL APPROVAL if Required

RECORD OF CHANGES/ADDITIONS

Change #	Change/Addition	Date of Change	Date Entered	Change By

FOREWORD

1. Authority: This Standard Operating Procedure (SOP) is issued under the authority of the JAFAN 6/0 Revision 1 and other applicable directives.

2. Office of Primary Responsibility (OPR): The OPR for this SOP is the ITT Program Security Office. Any inquiries concerning content or interpretation should be addressed to the OPR through program channels.

3. Format and Content: All provisions and requirements of this SOP apply to all personnel participating in programs within this facility. Each individual accessed to program information is ultimately responsible for its safeguarding. This SOP establishes the operating procedures derived from the JAFAN 6/0 Revision 1 and other applicable policy to assist you in protecting program information.

TABLE OF CONTENTS

LIST OF ATTACHMENTS

DEFINITIONS

1. **Access:** The ability and opportunity to obtain knowledge of program information.

2. **Acknowledged Special Access Program (SAP):** A Special Access Program whose existence is publicly acknowledged.

3. **Carve Out:** A classified contract issued in connection with a Special Access Program in which the Defense Security Services (DSS) has been relieved in whole or in part of cognizance responsibility.

4. **Codeword:** A single term assigned by the SAF/AAZ to a program or study. Codewords are classified IAW the security classification guides.

5. **Contractor Program Security Officer (CPSO):** An individual appointed by the contractor who performs the security duties and functions for Special Access Programs.

6. **Co-Utilization Facility:** A program-cleared facility at which one location elects to host the program-level work of another organization (e.g. NSA, DIA, etc.). In accordance with a signed co-utilization agreement, one organization acts as the Cognizant Security Authority (CSA) for both, in which specific responsibilities for each are agreed to in writing.

7. **Di/Trigraphs**: Two or three-letter abbreviations for handling systems (umbrella) or program codewords. These may be classified at different levels depending on the program's security classification guide.

8. **Government Special Security Officer (GSSO)**: An individual appointed who performs the security duties and functions for Special Access Programs.

9. **SMC/GPSE**: Security Office

10. **Handle Via Special Access Channels Only (HVSACO):** Handle within program channels only. It is used to identify unclassified information that requires protection in program channels. This means that the information does not have to be kept in a safe, but it must be treated as classified if it leaves the SAPF or when un-cleared personnel are present in the SAPF.

11. **Information Systems Security Officer (ISSO):** The provider-assigned individual responsible for the on-site security of the Information System(s) processing information for the program.

12. **Need-to-Know:** A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. Need-to-know demonstrates that denial of access to items of program information would cause inability to perform assigned duties in support of the program.

13. Operations Security (OPSEC): The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities.

14. Program Security Officer (PSO): The Government official(s) in a facility who administers the security policies for the Special Access Program(s).

15. Sensitive Compartmented Information (SCI): SCI is classified information concerning or derived from intelligence sources and methods or analytical processes that is required to be handled within a formal control system established by the Director of Central Intelligence (DCI).

16. Special Access Program (SAP): A program designated by the appropriate authority, under the authority of Executive Order 12958, for controlling access and distribution to protect particularly sensitive information. SAPs are established only when it is specifically shown that normal management and safeguarding procedures are not sufficient to limit must-know or access.

17. Special Access Program Facility (SAPF): A specific physical space that has been formally accredited in writing by the Cognizant Security Authority (CSA) or PSO which satisfies the criteria for generating, safeguarding, handling, discussing, and storing CLASSIFIED and/or UNCLASSIFIED program information, hardware, and materials.

18. Third Party Introduction: The program introduction of one program accessed individual to another program accessed individual by a third individual who has personal knowledge of the program accesses held by each of the first two parties. The third individual only introduces the first two parties at the common level of access held by each. An example would be, "This is a program (identify compartment(s) or study number(s)) introduction." Introductions must only take place within a SAPF.

19. Umbrella SAP: An approved DoD SAP that contains compartments for specific projects within the overall program. The nickname, program description, and accomplishments of each significant project will be reported in the annual SAP report.

20. Unacknowledged SAP: A SAP with protective controls that ensures the existence of the program is not acknowledged, affirmed, or made known to any person not authorized for such information. All aspects (e.g., technical, operational, logistical, etc.) are handled in an unacknowledged manner.

21. Waived SAP: An unacknowledged SAP to which access is extremely limited IAW the statutory authority of Section 119e of 10 U.S.C to include Congressional members. Unacknowledged Special Access Program protections also apply to Waived Special Access Programs.

ACRONYM LIST

ADPE	Automated Data Processing Equipment
AFCAF	Air Force Central Adjudication Facility
AFOSI	Air Force Office of Special Investigations
AFSPC	Air Force Space Command
CI	Counter Intelligence
CMB	Configuration Management Board
COMSEC	Communications Security
CPI	Critical Program Information
CSA	Cognizant Security Authority
CUA	Co-Utilization Agreement
DCC	Document Control Center
DCI	Director of Central Intelligence
DCS	Defense Courier Service
DIA	Defense Intelligence Agency
DSS	Defense Security Services
EAP	Emergency Action Plan
EO	Executive Order
FAR	Federal Acquisition Regulation
FOUO	For Official Use Only
FWAC	Fraud, Waste, Abuse & Corruption
GPM	Government Program Manager
GPSD	Global Positioning Systems Directorate
GSSO	Government Special Security Officer
HVSACO	Handle Via Special Access Channels Only
JAFAN	Joint Air Force Army Navy
JPAS	Joint Personnel Access System
LOCN	Letter of Compelling Need
NISPOM	National Industrial Security Program Operating Manual
NRO	National Reconnaissance Office
ISOO	Information Systems Oversight Office
OCA	Original Classification Authority
OPSEC	Operations Security
PAR	Personnel Access Request
PASS	Personnel Access Security System
PDA	Personal Data Assistant
PED	Portable Electronic Device
PIF	Personnel Information File
PIN	Personal Identification Number
PM	Program Manager
PR	Periodic Reinvestigation
PSO	Program Security Officer
PSQ	Personnel Security Questionnaire
RFP	Request for Proposal
SAP	Special Access Program
SAPCO	Special Access Program Central Office

SAPF	Special Access Program Facility
SAPIA	Special Access Program Indoctrination Agreement
SAPMO	Special Access Program Management Office
SCG	Security Classification Guide
SCI	Sensitive Compartmented Information
SEO	Security Education Officer
SGN	Secure Global Network
SIF	Security Information File
SIMS	Security Information Management System
SMC	Space & Missile Systems Center
SOP	Standard Operating Procedures
SSBI	Single Scope Background Investigation
SSO	Special Security Officer
SSP	Systems Security Plan
STE	Secure Terminal Equipment
SYSW	Space Superiority Systems Wing
TOE	Transfer of Eligibility
TSA	Transportation Security Authority
TSCM	Technical Survey CounterMeasures
TSCO	Top Secret Control Officer
VTC	Video TeleConferencing

CHAPTER 1

GENERAL PROVISIONS AND REQUIREMENTS

Section 1. Introduction

1-100. Purpose.

This Standard Operating Procedures (SOP) implements security policy found in applicable directives (i.e., JAFAN 6/0 Rev 1, AFIs, SAF/AAZ policy letters, etc.). All processes and procedures are implemented to prevent unauthorized disclosure of Special Access Program (SAP) information and to control authorized disclosure of classified SAP information (need-to-know).

1-101. Scope.

This SOP is the primary security policy reference for the ITT Clifton facility Special Access Programs. Conflicts between guidance in this SOP and other directives or regulations should be referred to your CPSO. Changes or updates to this SOP will be made as needed.

1-102. SAP Program Areas.

Areas NZ-09-021, Z-09-004, Z-09-042, Z-241, Z-242 are accredited for discussion, storage, and/or processing of SAP information. Our SAP facilities have current co-uses with various organizations which are kept on file with GPSD/ENS Program Security.

1-103. Waivers.

Requests for waivers to security requirements must be directed to the GSSO and processed using SAP Format 12. A waiver is any action that increases or decreases security requirements in the JAFAN 6/0. Waiver requests can only be approved by the AF Special Access Program Central Office (AF SAPCO). Every effort will be made to avoid waivers to policies unless it is in the best interest of the government. Convenience is not justification for a waiver request.

Section 2. General Requirements

1-200. Responsibilities.

Government SAP Security Officer (GSSO): Mr. Vernon Utley and Mr. Michael Kounter have been appointed as GSSO's. They exercise their authority on behalf of AFSPC/A8ZS (SAPMO).

b. Contractor Program Security Officer (CPSO). Mr. Thomas Oceanak is the ITT Clifton security representative responsible for the day-to-day security management of program(s) assigned to support a specific division or area. The ITT CPSO has been approved by the GPSD GSSO to give direction to contractor personnel on security related matters. Questions relating to individual programs should be addressed to the CPSO. Ms. Rosalie Brancatelli is approved as the Alternate Contractor Program Security Officer/ACPSO.

c. Security Organization. An organizational structure identifying different functions of the security organization and personnel assigned to those functions (Attachment 1).

d. Government Program Manager (PM). The Government PM has ultimate responsibility for all aspects of the program. He/she works with the GSSO/CPSO in administering the security requirements of the program. Involving the GSSO/CPSO at the inception of the program is critical to meeting and maintaining all security requirements.

e. Individual Program Personnel. Each program accessed individual is tasked with protecting SAP information in their possession. This includes everything from applying appropriate markings, disclosure, storage, reproduction, transmission, and destruction. This responsibility cannot be delegated to anyone else. Each program accessed personnel will receive an initial indoctrination briefing focusing on their security responsibilities.

1-201. Badge System.

a. Badge Control. Building entry badges are issued by the ITT Clifton Security Office. It is imperative you maintain positive control of your badge at all times. If you lose one of these badges, you must contact Security on 973-284-4537. If you forget your badge, visit the front lobby to request a temporary employee badge. They have a list identifying you as a ITT Clifton employee. The badge will only work for that day. Do not be afraid to challenge individuals you don't recognize or are not wearing a badge.

b. Badge Issue and Identification. Personal recognition is used in lieu of program badges within the program area. Because we use personal recognition, it is important that all accessed personnel challenge individuals they do not recognize as program accessed within the SAPF.

c. Escort Procedures & Visitor Badges. If you are expecting visitors that do not have their own facility badges, you must meet them in the lobby. The visitor will be issued an Escort Required badge or an Non Escort badge depending on what is known about the visitor. Visitors given Escort Required badges must be under your visual control at all times until you return the visitor to the lobby and return the badge. Visitors to the Program areas will sign in either the Program briefed or Non Program Briefed book. Non Program briefed visitors will be closely escorted and the program area sanitized.

1-202. Communications Security.

Secure Terminal Equipment (STE) phones in the facility are used for classified and unclassified calls.

a. Secure Communications. The STE's are procured and installed by the ITT COMSEC Responsible Officer (CRO)/Manager. All classified program information must be transmitted ***only*** by approved secure communications channels. ITT has non-secure and secure communications capabilities within the SAPF's.

b. STE Operations. Once a secure phone has been installed, it may not be moved to another location without **prior** coordination with the CRO. A unique KSV-21 Enhanced Cypto Card is issued with each STE. The KSV-21 must be removed when securing your office at day's end. It should be stored in your safe container. We do not have open storage so KSV-21 cards cannot remain in your phone. KSV-21s must be updated, as a minimum, on an annual basis. This can be done directly from your phone following the menu prompts. Contact the CRO if you require this information. Speakerphone capability is allowed on a case-by-case basis. The CRO/Security will be notified prior to meeting and the individual holding the meeting will set the level. Speakerphone approval is file with Program Security.

(1) Once the called party answers and you've established voice recognition, **go secure immediately prior to any program discussions**. Do not attempt to "talk around" sensitive or classified information. By going secure, you are precluded from revealing classified information and committing a security infraction, potential violation or compromise of classified information.

(2) While waiting for your party to come on the line, be aware of background conversations. If you work in an area with many people and little space, lower the volume of your conversations or conduct the classified discussions behind closed doors. If you need to leave the phone during the course of the conversation, put the phone on hold or mute. ***Never*** leave the phone off-hook without the hold button depressed. Background conversations are easily overheard and/or intercepted.

(3) When placing a call, particularly when your office door is open, say "phone up," "non-secure line," or "placing a call." This will advise those around you that your phone is "live" and conversations can be overheard. When you've completed your call, say "phone down" or "call is terminated."

(4) Make sure the phone is properly on-hook after each use. It is common for the handset to be quickly put down and not sit properly in the cradle. Take the extra second to guarantee the phone is on-hook.

(5) Any problems with STE operation should be immediately reported to the CRO/COMSEC Manager Tom Oceanak.

c. Voice Mail. The Voice Mail feature is available on The ITT Corporation's phone system. In order to preclude someone from within or outside the program area reading your voice mail messages, it is critical that you **NOT** use as your 5-digit password, a number combination that reflects your extension number (last four digits of your phone number). Three failed attempts to enter your correct password will lock you out. Passwords to your voicemail must be changed as directed by the Manager Security. <u>No</u> classified information can be left on the system or your voice mail header. Classified Information recorded on the phone system must be reported to the IAM immediately on x4237.

d. Telephone resources are for "Official Use Only". Official use also includes calls deemed necessary in the best interest of the corporation. If your phone may be monitored at any time by company officials

e. Secure Video Teleconferencing. We have one Video TeleConferencing (VTC) encrypted systems for classified meetings located in Z-09-042. In order to schedule a VTC, you must first reserve the conference room through the Security staff within the Clifton facility then e-mail the VTC coordinator to set the time and date. Provide the VTC Coordinator your name and phone number, level of the meeting, and locations (facility ID's) which will be attending the VTC in the e-mail. If you include a purpose of the meeting, make certain it does not contain classified information. Contact program security on the day of the meeting to set the level and ensure that all attendees are appropriately briefed to the material being discussed.

f. Speaker Phone-Secure Communications. ITT Clifton is approved for the use of STE secure speaker phone in all SAPF rooms. If you have a need for use speakerphone capability follow these steps:

1) Contact program security and inform them of your intention and time. Security will temporarily enable the Secure Speaker Phone.
2) Close the SAPF room door and remove the KSV-21 from the safe.
3) One the KSV is inserted, dial the number to the appropriate party(s)
4) Acknowledge individual on receiving end.
5) Initiate secure voice feature.
6) Confirm all parties are in the secure mode.
7) Enable speakerphone and hang up the handset.
8) Set the level of the discussion/meeting.
9) User is responsible to ensure conversation stays at the appropriate level.
10) When call is completed, user is responsible for terminating the call and returning the KSV to program safe and placing it in the correct folder. Security will disable the Speaker Phone after the call.

1-203. Security Inspections.

a. Government. Periodic security inspection/oversight ensures personnel are knowledgeable of program management policies and procedures in addition to evaluating how well we've translated security policy into program security procedures. GPSD will conduct security inspections of ITT Clifton approximately as required. These inspections can be announced or unannounced.

b. Self-Inspections. ITT Clifton conducts an annual self-inspection of our documentation and procedures using the JAFAN 6/0 Inspection Checklist. All functional areas are reviewed. Deficiencies identified and documented during the self-inspection will be reported to the GSSO through the CPSO. Corrected or a corrective action schedule will be developed to correct any deficiencies.

Section 3. Reporting Requirements

1-300. General.

All individuals are required to report information/incidents that may impact their continued eligibility to possess a clearance or access to the CPSO/ACPSO or personnel security representative. This information includes, but is not limited to, association with non-US citizens, financial issues, reports of self-initiated alcohol, drug or mental treatment, reports of administrative disciplinary action, and civil or military arrest/charges These reports will determine whether the situation/incident is serious enough to warrant removal of your access. There are two options: suspension and revocation. See Section 2-203 of this SOP for further descriptions.

1-301. Security Violations and Improper Handling of Classified Information.

a. Security Violations and Infractions.

(1) Security Violation. A security violation is any incident that involves the loss, compromise or suspected compromise of classified information. Examples of this could be: discussing classified over a non-secure line or losing classified program information. Security violations must be reported to the CPSO immediately upon discovery or occurrence then reported to the GSSO/PSO within 24 hours by the CPSO/ACPSO.

(2) Security Infraction. A security infraction is defined as any other incident that is not in the best interest of security, but does not involve the loss, compromise or suspected compromise of classified information. Some examples of infractions are: leaving classified information on a whiteboard, failing to secure a safe container, or improperly removing classified from the SAPF (provided the material never left control of the person and was returned, secured or destroyed IAW with approved methods). Security infractions must be documented and the report provided to the CPSO within 24 hours.

(a) Security infractions can be significant or minor. Normally the significant infractions would involve an individual who commits a continuous string of infractions that could lead to potential compromise. A minor infraction is considered a deviation from standard security practices with no probable compromise of program information. The following rules apply for significant infractions:

1 For ITT and ITT contractor personnel, forward your report to the CPSO. A determination will be made if a report should be made to the individual's supervisor for administrative or disciplinary action.

4 All reports of security violations and infractions will be recorded at the Confidential/HVSACO or lower level, if possible and filed in the individual's Security PIF.

The PERSEC staff and CPSO use the data to determine trends by identify training needs; identify individuals that need additional training, or worst case, document that a person should not be trusted with protecting classified information.

b. Inadvertent Disclosures.

All inadvertent disclosures (e.g., involuntary unauthorized access) to program information by an individual without any program access, or an accessed individual not possessing a particular access, will be reported to the CPSO who will report to the GSSO. The extent of the exposure will be evaluated to determine if the individual should complete an Inadvertent Disclosure Oath on SAP Format 5. If, during emergency response situations, guard personnel or local emergency authorities (e.g., police, fire, medical, etc.) inadvertently gain access, they will be required to complete a SAP Format 5. Refusal to sign SAP 5 will be reported to the GSSO/PSO immediately.

c. Inquiries and Investigations.

(1) Preliminary Inquiries: Upon discovery or report of a security violation, you must immediately notify the CPSO. The CPSO will immediately review the circumstances surrounding the incident. If there is a potential for loss or compromise, a preliminary inquiry will be conducted as soon as possible and the GSSO will be notified by the CPSO.

(a) If the preliminary inquiry is not sufficient to resolve the security incident, then a formal investigation will be initiated with the investigation official being appointed by the ITT Security Manager.

(b) A disinterested individual, not assigned to the office where the incident occurred, will be appointed as the Investigating Official. Individuals involved in the incident will be interviewed to gather information regarding the violation. A report (memo form) will be prepared by the Investigating Official and submitted to the CPSO, Manager Security and the GSSO/PSO.

(c) If the preliminary inquiry determines that a "possible compromise" or "compromise" has occurred, the following minimum actions will be taken:

1 The GSSO/PSO and will be verbally notified within 24 hours.

2 An initial written report will be forwarded via secure means by the CPSO to the GSSO/PSO within 48 hours of appointment of the Inquiry Official. Both verbal and written reports will include:

3 Date/time/place the violation occurred.

4 Who discovered the violation?

5 Complete information on content and type of classified information involved in the violation.

6 Identity of all persons known to be involved in the violation at the time of the report.

7 Summary of circumstances surrounding the incident as known at the time of the report.

8 The ITT Manager Security will appoint an individual as an investigating officer within 24 hours to conduct a formal investigation. These procedures are:

9 The appointed individual will not have any actual or perceived conflict of interest with the matter or individual being investigated.

10 The individual's appointment letter will fully explain the matter to be investigated and pertinent regulatory guidance.

11 The Inquiry Official will pursue the investigation full time until completed and released by the appointing official.

12 Program management will ensure that all personnel who might contribute to the investigation are made available to the investigating officer.

13 When the investigation is completed, the Inquiry Official will prepare a final report. The report will include corrective action and/or discipline imposed on culpable individuals.

14 Determine if personnel suspensions are appropriate.

d. Fraud, Waste, Abuse and Corruption (FWAC). In order to protect program information, separate FWAC reporting procedures have been established. **DO NOT** use other advertised FWAC hotlines when making a report. If you have a FWAC report to file, follow these procedures:

(1) Call the FWAC Hotline at 800-488-9010 (active from 0700-1700 EST, Mon-Fri). This number is posted in the program facility, is a secure phone (with unclassified only voice mail), and answered by program- accessed personnel. The Poster with the number is posted in all ITT SAPF's.

CHAPTER 2

SECURITY CLEARANCES

Section 1. Facility Clearances

2-100. General.

ITT Clifton facilities are accredited for up to Top Secret/SCI/Special Access Required. Our SAPF's are under SAF/AAZ cognizance and our SCI Cognizant Authority is DIA.

2-101. Defense Security Services (DSS).

DSS does not have any special programs that DSS holds cognizance here on site.

Section 2. Personnel Clearances and Access

2-200. General.

a. Personnel security requirements are established in accordance with JAFAN 6/4. JAFAN 6/4 outlines the procedures used for determining access eligibility to SAPs. Access to program information is neither a right nor an entitlement; it is a wholly discretionary security determination granted only to those individuals possessing a "need-to-know" and who meet stringent background and security standards.

b. Transfer of Eligibility (TOE). The TOE allows an individual's eligibility for access to SAPs be transferred from one DoD component or contractor to another, not the SAP accesses. The TOE is negotiated between the losing and gaining organizations. The SAP Format 32 (TOE Request Form) is used for this purpose. The following guidelines allow a TOE to be accomplished:

(1) Individual's clearance must be currently active and SSBI current or a Periodic Reinvestigation (PR) submitted prior to the expiration of the last investigation.

(2) Individual must have been previously SAP accessed without a Waiver.

2-201. SAP Access Procedures.

a. The individual must possess a valid "need-to-know" and materially and directly contribute to the program. Program access is not granted to anyone merely by reason of federal service, contracting status, or as a matter of right or privilege based on title, rank or position. The Program Manager (PM) is responsible for making this determination. Personnel Access Requests (PARs) should be closely scrutinized to validate that only those accesses required are requested for approval.

b. In order to be eligible for access to GPSD Programs, the candidate must possess a final clearance based on an appropriate investigation for the level of access required. All investigations must be current within the past five years. This requirement can only be waived by the AF SAPCO. If the candidate does not meet this criteria, then the following actions must be taken: 1) Periodic reinvestigation update has been initiated (case has been opened), and 2) the Program Manager must submit a letter of compelling need (LOCN) through SMC/GPES justifying why a waiver to program requirements is critical to mission accomplishment. This LOCN must be endorsed by the GPSD Program Manager and the GSSO. OR – the PSO may approve eligibility provided there is no derogatory information and the request for a Periodic Investigation (PR) was submitted prior to the expiration date of the last investigation.

c. The candidate must agree to submit to a CI-scope polygraph at any time during the period of their program access.

2-202. Program Access Requests and Tier Review Process.

a. Access Quota Systems.

Program accesses are managed with an access quota system. This system controls the total number of accesses available to GPSD for each program. The ceilings are integrated into a government system to prevent exceeding the quota ceiling. Not all personnel working within ITT Clifton Special Access Program are accessed to the same programs; therefore, it is imperative that a third party introduction is obtained prior to release of information to other ITT Briefed personnel. If you do not know an individual's accesses and need to discuss program data with them, contact the CPSO/ACPSO/PERSEC.

b. Initial Nomination

Once the candidate is identified, the Program Manager (PM) or his/her designee will coordinate with the CPSO and Personnel Security to prepare a Program Access Request (PAR). The PM is responsible for supplying a justification for access. Need-to-know is determined by the PM. Each PM will sign the PAR on line 27 if they are the requestor. The PAR Process Checklist, (Attachment 2) will be followed when submitting a PAR.

c. Candidates with current investigation (ANACI/NACLAC/SSBI/SCI).

(1) The GSSO can approve program eligibility of the candidate when all of the following criteria are fully met:

(a) The case contains no waivers or warnings from the cognizant SCI authority. (Applies only to candidates already possessing SCI eligibility.)

(b) Candidates must submit a SF 86 that has been updated within one year. If required, the candidate must make necessary changes, re-sign and re-date. The SF 86C can be used to submit the changes with the SF 86 in lieu of making changes directly on the SF 86.

(c) JAFAN 6/4 is used by ITT Clifton Personnel Security to determine SAP Tier eligibility.

(2) All nomination packages not meeting Tier 1 criteria will be sent to the GPSD for Tier 2 adjudication. Access denials are ONLY made by the Chief, SAF/AAZ. GPSD/ENS Personnel Security will be notified of the denial and the AFEDS will reflect the denial. Upon request, the candidate's CPSO or company will be forwarded a statement explaining

the basis of the adverse decision. The owning organization may appeal the adverse eligibility as directed.

d. Additional Access(s).

(1) The ITT CPSO will validate continued security eligibility. PARs for additional accesses require complete justification for access in Block 25. The Program Manager or requestor must validate "need-to-know."

e. SCI Access. SCI access is required in conjunction with certain program access. The following action will be taken. The ITT CPSO will verify the SCI eligibility using the Joint Personnel Access System (JPAS) prior to allowing access to SCI data. Personnel are nominated for SCI to the SMC/SSO for approval.

f. Access Approval. Final access approval is a three-step process. The first step is the candidate's "need-to-know" determination by the Program Manager. It requires completion of a PAR. The second step is verification that an available access quota exists for the candidate. The third step is the formal determination of the candidate's security eligibility. Each candidate must be adjudicated to JAFAN 6/4 standards.

2-203. Suspension and Revocation.

When time is of the essence, GSSO/CPSO is authorized to verbally suspend a person's access. Unless unusual conditions prevail, the Contractor Program Manager will be provided written confirmation of the verbal direction no later than the next working day. **Suspension of access** is an action taken regarding a currently accessed individual as a result of certain personnel security conditions or questionable circumstances. Suspension is designed to allow time to collect pertinent information to determine if an individual's access should be revoked, whether to create a Security Information File (SIF), or whether to return the individual to his/her normal duties. The action is temporary, but access cannot be reinstated until a full review of the details and a formal AFCAF re-adjudication of the individual's eligibility is completed. **Revocation of access** is taken when an individual with current access is formally determined to be ineligible for access after receipt and review of new or additional disqualifying information. Due process and appeal notification procedures are required if the individual is formally determined to be ineligible for access as a result of this action.

2-204. Periodic Reinvestigation (5-Year Update).

All personnel should be aware of the date they should coordinate the initiation of their periodic reinvestigation with their Personnel Security Office. The initial process should begin six (6) months prior to the five-year anniversary of the date of your current background investigation. Your completed periodic reinvestigation cannot be submitted sooner than six (6) months prior to that date or e-QIP will reject it.

2-205. Counter-intelligence (CI) Polygraph.

Due to the sensitivity and criticality of the program information, a random CI-scope polygraph is a program requirement. At any time during an individual's access, they can be required to take a polygraph. Questions regarding the polygraph should be addressed to GPSD/ENS Personnel Security or GSSO.

2-206. Security Records.

A Personnel Information File (PIF) is maintained in the ITT Clifton SAP Personnel Security office for each program accessed individual and some on-site contractors or any contractor that does not have an accredited facility over which ITT Clifton has cognizance.

CHAPTER 3

SECURITY TRAINING AND EDUCATION

Section 1. Security Training and Briefings

3-100. General.

All individuals accessed to program information must participate in the security training program. ITT Clifton has a designated Security Education Official (SEO) Tom Oceanak who is primarily responsible for administering the security education program. The SEO is responsible for developing the formal training program, and providing materials, training guides, instructional aids, etc. **Supervisors and managers, at all levels**, are responsible for ensuring their personnel attend and participate in this training.

3-101. Security Training.

The following training is required of all individuals having access to program information:

a. Initial SAP Indoctrination. The initial indoctrination will provide the individual the security requirements for the program ensuring he/she understands their particular responsibilities. Initial program indoctrinations are conducted by the CPSO/ACPSO as required and lasts approximately (2) hours. Personnel will be required to sign a SAP Indoctrination Agreement (SAPIA Format 2) before classified information is revealed to them. Failure to complete this form will bring the indoctrination process to an end, and the GSSO will be notified immediately.

(1) Direction to read the Standard Operating Procedures (SOP) and IS General Users Guide (Attachment 4) will be provided to the newly indoctrinated individual following the briefing. These individuals will sign statements that indicate they understand the procedures and accept responsibility for adhering to them.

(2) Initial indoctrination training will include all subjects identified on SAP Format 17.

b. SCI Indoctrinations. SCI indoctrinations are conducted as required by the Prime's CSSO.

c. Additional Access Briefings. When an individual is approved for additional program accesses, they should contact the Security Education Officer (SEO) to schedule the briefing.

3-102. Refresher Briefings.

ITT Clifton conducts annual refresher training to meet program requirements. All SAP-accessed, local personnel sponsored by ITT Clifton must complete this training. Training may also be supplemented with email notices, newsletters, bulletin boards, etc. This training covers information listed on SAP Format 17 and personnel will be provided the following information as a minimum:

(1) Updates or changes in policy/procedures.

(2) Review of requirements included in the Indoctrination Agreement.

(3) Foreign intelligence techniques and threat updates.

(3) Adverse and personal information reporting requirements.

(5) Common security deficiencies discovered during our latest security inspection or our own self-inspection.

3-103. Debriefing and/or Access Termination

a. If you no longer require access to program information, you will be debriefed by the CPSO/ACPSO. This occurs when an individual no longer meets "need-to-know" criteria (PCS, reassigned, retirement from company, etc.). Access is also terminated in the case of a suspension, when the individual no longer meets security requirements for SCI or program information.

b. Prior to debriefing, you must contact the CPSO to obtain a listing (inventory) of your classified holdings. Request this information with sufficient time to reconcile your holdings prior to your scheduled debriefing as this inventory must be completed before your debriefing can occur. **If you are unable to reconcile your inventory, it will delay your debriefing and your departure.**

c. You will execute a debriefing acknowledgement at the time of your debriefing. The debriefing will, as a minimum, remind you of your continuing obligations to protect the classified information and that the Indoctrination Agreement is a legal, binding contract between you and the US government. Applicable espionage laws will be made available to you during the debriefing. All visit/perm certifications in effect at the time of the debriefing will be cancelled.

3-104. Personnel Security Reporting Requirements.

a. **Changes in Status.** Each accessed individual must also report changes in their status. These changes should be provided in written form to your CPSO or a ITT Clifton Personnel Security Representative. Changes requiring reporting include but are not limited to:

(1) Changes to your PSQ (SF 86) to include marriage/divorce/cohabitation. All marriage, legal separation, divorce, and cohabitation (bound by ties of affection/obligation) must be reported. If you have intentions to marry a foreign national, notify GPSD/ENS in advance of your planned marriage or you risk suspension of your access until the impending spouse can be investigated. Foreign national roommates, relatives, etc., must be reported on SAP Format 20, SF86, SF86C and E-Qip.

(2) termination of employment,

(3) alcohol abuse, illegal drug use, or abuse of prescription drugs,

(4) change in citizenship of family members,

(5) financial difficulties (wage garnishment, repossessions, collection accounts, etc.) and sudden wealth (lotteries, inheritances, etc.),

(6) law violations and traffic tickets of $500 or more,

(7) Legal involvement (defendant or plaintiff),

(8) health-related concerns, mental or physical except counseling related to marital, family, or grief issues (unless related to violence by you or drugs are prescribed). Also excludes counseling for adjustments from service in a military combat environment.

(9) Security infractions, violations or inadvertent disclosures.

3-105. Foreign Travel/Contacts.

a. **Foreign Travel.** Program accessed personnel must submit a foreign travel notification form SAP Form 6 to the CPSO or Personnel Security, 40 days **prior** to all travel outside the continental United States, Hawaii, Alaska and the U.S. possessions (i.e., Puerto Rico, U.S. Virgin Islands, Guam, etc.) with the exception of Mexican and Canadian border towns for one-day visits (not overnight stays). The one day travel to Mexico or Canada must be reported on your first duty day back to the office. SAP Format 6 must be used for reporting foreign travel. If you report your foreign travel to another customer on a different form, that form is acceptable as long as it contains all required information. All other required reporting is your responsibility to make directly to other offices. Foreign Travel to a country listed on the Security Threat List (STL) must be reported to the CPSO through Program

Channels 40 days prior to travel being under taken. Leisure travel to STL countries must be approved by the PSO or risk debriefing if you decide to go anyway.

(1) Foreign travel notifications are filed in your Security Personnel Information File (PIF) and entered into the AFEDS by the government.

(2) Defensive foreign travel briefing requirements are covered in Section 3-105.b.(1).

b. Foreign Travel Briefings. Individuals receive a foreign travel security briefing at least annually as part of the refresher training. When you submit a foreign travel notification form, your record will be checked to verify if you've received this briefing within the past year. If not, you must receive the training prior to your travel. Contact the SEO when you return from travel to close out your foreign travel report. Incidents considered threatening or suspicious encounters with foreign nationals must be reported when you return. Deviations from your submitted itinerary must also be reported. These questions are noted on the back page of SAP Format 6.

(1) The ITT Clifton CPSO/ACPSO/PERSEC provide travel briefings as required.

c. Foreign Contacts. Program personnel must complete SAP Format 27 and submit it to the ITT Clifton personnel security representative to report foreign contacts whether they occur within or outside U.S. borders. Foreign nationals include anyone who is not a U.S. citizen. <u>Casual contact that does not go beyond common courtesy or normal business practices need not be reported</u>. If unsure contact a security representative to answer questions about what needs to be reported. Foreign Contacts meeting the following criteria ***must be*** reported:

(1) Contact with personnel from foreign diplomatic establishments;

(2) Information containing actual or potential terrorism, terrorist groups, espionage or sabotage of any U.S. facility, activity, person or resource;

(3) Recurring contact with a non-U.S. citizen when financial ties are established or involved;

(4) A request for illegal or unauthorized access to classified or controlled information;

(5) Contact with an individual (**regardless of nationality**) under circumstances that suggest you may be the target of an attempted exploitation by the intelligence services of another country.

(a) Report social contact when:

1) You are questioned regarding specifics of your job, organization, mission, etc.;

2) Questioning is persistent regarding social obligations, family situations, etc.;

3) Frequent or continuing contact is anticipated (e.g., pen pals, Internet, ham operators, student study groups, housekeepers, exchange students, etc.);

4) Any unusual incident with a citizen or other entity of a foreign country.

CHAPTER 4

CLASSIFICATION AND MARKINGS

Section 1. Classification

4-100. Classification Management.

a. Quality classification management is essential to maintaining the integrity of program information and preventing compromise and/or unauthorized access.

b. The Senior program scientists/engineers and serve as the overall Classification Managers on individual program information within their area of responsibility. In their absence, your program CPSO is available to answer questions or provide clarification.

c. Individuals generating program documents or information **are responsible for ensuring proper classification** of all information contained within by following the guidance in the Security Classification Guides (SCG)s. Contact your Security Education Officer (SEO) to obtain required SCGs.

4-101. Security Classification Guidance. Each SAP has a SCG that identifies Critical Program Information (CPI). ITT Clifton has derivative classification authority, not Original Classification Authority (OCA). Become familiar with the SCGs for programs you support. Classify <u>each document and/or portion mark</u> on the basis of the information it reveals or contains.

4-102. Nicknames, Code words, and Other Program Identifiers. Special access programs are identified by a two-word nickname (umbrella or parent) and assigned a digraph and/or a codeword (known as a trigraph or child). Nicknames and code words can be classified. SCGs will provide this classification information. Digraphs and trigraphs should not be released outside SAP channels.

4-103. DD Form 254 Requirements.

a. A DD Form 254 is issued to all program contractors that is specific and comprehensive in identifying all security procedural and classification specifications. DD254s are issued beginning with the RFP process of classified efforts. Contract work cannot be issued to a contractor without an approved/signed DD254.

b. If a DD Form 254 is classified because of program information, it must be protected within SAP channels.

4-104. Changes, Challenges, and Reviews.

a. You should submit change recommendations or challenges to security classification to the GSSO through your CPSO. If you have a substantial reason to believe information is improperly or unnecessarily classified, your CPSO will notify the GSSO. Identify to him/her, in writing, the reasons you believe the information is improperly classified. If necessary, the GSSO will coordinate with the Cognizant Security Authority for the SCG.

b. You **cannot** declassify information as a result of official publication (issued outside program channels), public disclosure, or inadvertent or unauthorized disclosure of identical or similar information. If possible, notify and provide a copy of the information through your CPSO to the GSSO through secure channels.

4-105. Coversheets. Coversheets **must be** affixed to all classified material (including working papers) that are created, printed, reproduced via copier, or distributed. You must write the program digraph/trigraph(s) contained within the document on the coversheet. NOTE: CLASSIFIED HANDLING SYSTEMS OR CODEWORDS WILL NOT BE SPELLED OUT ON COVERSHEETS. It is also advisable that you affix coversheets to U/HVSACO material. Standardized coversheets provided by GPSD are available from the CPSO. Do not affix SAP coversheets to collateral or SCI-only information. This material must contain the appropriate coversheet.

4-106. Top Secret Access Records. All Top Secret material must have a Disclosure Record affixed to it. Our TS coversheets incorporate this requirement. The first time you access a Top Secret document (controlled or working papers), you must sign and date the coversheet/access record. You need only sign the access record once regardless of the number of times the access occurs. Access records are affixed to the destruction certificate and filed with this certificate until it is destroyed after five years.

Section 2. Marking Requirements

4-200. General.

a. DoD 5200.1-R/AFI 31-401, and JAFAN 6/0 provide the basic marking guidelines for classified program material except as modified below. If there is doubt as to the classification of a particular document or information, the highest level and most restrictive category of marking and identification will be used in order to ensure proper protection of the information. This is, however, an interim protective measure until a conclusive determination is made using the appropriate SCG(s).

4-201. Program Specific Markings. Program material will be marked and controlled using guidance IAW the JAFAN 6/0, SCGs, SAP Marking Guide, and other guidance as directed by your PSO. The SAP Marking Guide can be found in some SAPF's any by contacting your CPSO. Specific information required on the title page or internal pages of a SAP document include:

a. Top Secret Control Numbers.

(1) Control numbers will be applied to all Top Secret material faxed or couriered outside the SAPF. The control number will appear in the upper right corner on each classified page of a document to include the title page.

(2) Top Secret control numbers will consist of the following in sequence:

(a) YY - last two digits of the year of origination.

(b) NNNN - a sequential number assigned to documents created during a given calendar year. Example, 09-0001 would be the first document created in 2009.

b. Page numbers. Even though page numbers are required only on Top Secret accountable material, it is strongly recommended that you apply page counts to all levels of information. The total page count is required on fax and document receipts and it also allows the holder of the information to determine if a page is missing. Page numbers must be in the following format: "Page (#) of (total pgs)." Whenever possible, they should be affixed in the bottom right corner of the page.

c. Copy numbers. Copy numbers will be displayed on the title page or first page of every accountable document (i.e., Top Secret documents). The annotation will reflect "Copy (#) of (total)." If additional copies are generated from an original copy (i.e., Copy 6), the additional copies would be Copy 6A, Copy 6B, etc.

d. All program documents will have the overall classification at the top (header) and bottom (footer) of each page. Compartment codeword will appear at the top (header) and bottom (footer) of the page and the handling system, in addition to Special Access Required.

SECRET/(Codeword(s) or Trigraph(s))XXX/XXX/XXX
XX (Digraph or Umbrella) Special Access Required

It may be necessary to mark the material with multiple handling systems (i.e., SAP, SCI, etc.). You have the option of marking each page according to the classification of that specific page or to mark each page with the highest classification of the information contained in the entire document (overall classification). Portion marking is required on all program documentation as specified in para 4-202 and the Program Marking Guide. Engineering Notebooks are exempt from portion marking (see Section 5-204).

e. Examples of how to appropriately mark pages containing multiple handling systems, magnetic media, etc. can be found in the Program Marking Guide located in the ITT Clifton Program Security Office.

4-202. Portion Markings. Each section, part, paragraph, title, table, figure or similar portion of a classified document must be marked to show the highest level of its classification. Both classified and unclassified paragraphs will be marked. Classified SAR paragraphs will be marked with the classification abbreviation (i.e., C, S, TS) and the appropriate program digraph, trigraph, or SAR, as required.

4-203. Component Markings. The major components of complex documents are likely to be used separately. In such cases, each major component will be marked as a separate document. If a cover letter is prepared for forwarding or distributing the classified material, it will be marked with the highest overall classification of all the attached material with appropriate downgrading notation when attached material is removed.

4-204. Warning Notices.

a. Use of warning notices is intended to enhance a holder's ability to provide additional protective measures or to further restrict access to the information.

b. The marking, "Unclassified/Handle Via Special Access Channels Only," identifies information that must remain within SAP program protective channels. This material can be sent via First Class Mail to post office boxes. It must be destroyed as classified waste. Additional information on marking and handling U/HVSACO material can be found in Appendix A of the JAFAN 6/0 or the Program Marking Guide.

c. Media Markings.

(1) Removable magnetic media will be marked with stickers affixed to the media. DCC personnel issue magnetic media and affix the classification stickers. Due to the limited space available on a media label, the digraphs and SAR, to identify the trigraphs, can be used. In most cases, each piece of magnetic media will be marked with a separate, distinct control number and each piece of media is Copy #1. An example of an exception to this would be making ten CDs containing the same information and the CDs are not rewriteable. These CDs could contain the same number and be Copy 1, 2, 3, etc.

(2) All other program classified material will have the same descriptive information as in para 4-201 conspicuously stamped, printed, written, painted, or affixed by a tag, sticker, decal, etc.

4-205. Files, Folders, Binders, Etc. Files, folders, binders, envelopes, or other items containing classified documents, when not in secure storage, will be conspicuously marked with the highest classification of any material contained therein. Marking will be on the front and back, as a minimum. Coversheets can be affixed to meet this requirement. Coversheets can be obtained from the CPSO.

4-206. Transmittal Documents. A transmittal document will be marked with the highest level of classified information contained within or attached. It will include a notation to indicate the transmittal document's classification when the enclosures are removed. An example would be: "Letter is classified CONFIDENTIAL/XXX when enclosures or attachments are removed." This example assumes the enclosures or attachments would be SECRET and the transmittal letter only CONFIDENTIAL.

4-207. File Exemption Series.

a. Classification markings for program information will follow the guidance contained in Executive Order (EO) 13526 and Information Systems Oversight Office (ISOO) Implementing Directive No.1 dated Sep 22, 2003. Personnel in ITT Clifton are authorized as derivative classifiers only. Derivative classifiers will place the following information on the face of each classified document or other media.

(1) "Derived From" line identifies the source document(s) used to apply the classification markings. The source document is normally a SCG, but could be a report, letter, etc. If more than one source document is used, the term "multiple sources" can be applied. A listing of the multiple sources can be kept with the file copy or identified within the document. Additional examples of derivative markings can be found in the Marking Guide located in the ITT Clifton Program Security Office.

(2) The second line of the derived/declassification instructions will contain the "Reason." This information can be derived from the SCG or the reference document being used.

(3) The third line will contain the "declassification instructions." The "declassify on" date to be applied will be 40 years from the date of the document being generated. The declassify on date will be followed with the "Review On" date that will be six months prior to the declassification date.

(4) The fourth line will reference the authority for the 40-year exemption for declassification.

(5) An example of the derived from/declassify on instructions is shown below:

Derived From: XXX SCG (date of SCG) or Multiple Sources
Reason: EO 13526, Section 1.4 (will normally be (a) and/or (c)) – from SCG
Declassify On: 40 years from date of document generated
Review On: 6 months prior to declassification date
Authority: File Series Exemption dtd 30 Mar 2005

CHAPTER 5

SAFEGUARDING CLASSIFIED INFORMATION

Section 1. General Safeguarding Requirements

5-100. General. SAP classified material must be appropriately stored and locked in a GSA-approved safe container when the facility is not manned or when it cannot be protected visually from un-cleared visitors. Unclassified/HVSACO material must be protected visually (desk drawer, filing cabinet, etc.) from un-cleared visitors. The only exception to this would be during an emergency evacuation.

5-101. Clean Desk Policy. A "clean desk" policy must be implemented in all program areas. This is to ensure **all** classified, U/HVSACO and FOUO material has been properly secured and your work area is neat and uncluttered. Neat and uncluttered is further defined as no loose papers left on top of desks, filing cabinets, safes, tables or other surfaces. This procedure will preclude requiring the end-of-day checker from digging through material to be certain no classified material is left unsecured. U/HVSACO and FOUO may be stored openly or out of sight in desk drawer, file cabinet, etc. If stored openly, it must be protected from sight by non-accessed individuals.

5-102. Facility Access Controls. Entry into the ITT SAPF's are as follow:

a. SAPF's 287, 241, 242, 004, 042
For entry into these SAPF's we utilize Kaba Mas X09 locks, UL approved ADT IDS and Securetron DK2FSF digital entry Ciphers.

b. SAPF 021,020
For entry into these areas we use Kaba Mas X09 locks, UL approved alarm systems and ADT card access readers which the user swipes their badge and enters their unique pin to enter the facility.

5-103. Building Access. Access to the Clifton facility is as follows:

Each employee is provided a proximity card which acts as the company identification badge. This Prox badge allows entry to authorized doors around the facility. This ID badge will not open SAPF 21 and 20 unless it has been programmed to do so by the CPSO.

5-104. Program SAFPs. ITT Clifton has designated areas approved for discussion, storage and processing of SAP information within the facility. SAF/AAZ is the cognizant authority for our SAP areas and SAF/AQL has a co-use agreement with SAF/AAZ for the two SAP's.

5-105. Common Use Area Access. We have no common use area accesses.

5-106. Unescorted Access. Only appropriately accessed individuals will have unescorted access to the ITT Clifton SAP areas. All others will be under close constant escort.

5-107. After-Hours Access. A valid ITT Clifton badge to gain access after hours. To gain access to each program facility, an individual must be on the approved access list to gain access. Individuals working after hours must sign the after hours log which is located at the main entrance of each program facility. The business hours for the Clifton Facility are 07:00-19:00. Working hours for the 020 and 021 SAPF's are 24/7.

5-108. Hallways, Windows, Doors and Restrooms.

No classified discussion is allowed outside the SAP facility. There are no windows or internal restrooms in any ITT Clifton SAP facilities.

5-109. Facility Opening/Securing Procedures.

Only individuals accessed to all programs are authorized to open/close the SAPF designated by the CPSO. A listing of individuals authorized to Open/Close the area is posted on the back of each SAPF Door.

Individuals will be trained prior to being authorized to open and close the area. This training will include but is not limited to: the opening/closing procedures described below, along with the visitor process (posted in the interior of area above visitor log books), along with restrictions for giving out the combination.

SAPF Openiug:

1. The program cleared individual will unlock the SAPF by dialing the X09 lock combination on the entrance door.
2. The program cleared individual will then enter the Cipher lock code or swipe their badge and enter their PIN depending on which SAPF they are trying to access. Reference 5-102 a. and b.
3. The program cleared individual will then disarm the intrusion detection system (IDS).
4. The program cleared individual will then fill out the SAPF Open/Close Checklist with the date, his/her name, and the time.
5. The X09 will remain in the open position while the SAPF is occupied

SAPF Closing:

1. When closing the SAPF at the end of the day or when the SAPF is unoccupied, the exiting personnel will make a physical check of the SAPF area to ensure no material has been left out, and safes are secured. The exiting personnel will follow the End of the Day Check List posted by each door; complete the Safe Container Check Sheet and the SAPF open/close sheet.
2. The exiting program cleared personnel will then enter the alarm code to arm the intrusion detection system and immediately exit the room ensuring the door is completely closed tight swiping their badge as necessary.
3. The program cleared personnel will lock the SAPF by spinning the X09 lock on the entrance door and noticing that the alarm LED light has turned RED.

Section 2. Control and Accountability

5-200. General. The focus of accountability for program information is on strengthening the protection of magnetic media and the reduction of the amount of paper holdings within our SAPF.

5-201. Program Material Tracking System. TOP SECRET program material is assigned a control number and entered into the Log Book. The CPSO will assign control numbers to all accountable items. SECRET and CONFIDENTIAL hard copy documents need no formal accountability. However, these items are entered into a security log book for tracking purposes. In addition, transfer receipts are issued when transmitted outside the facility. Authorized, unclassified magnetic media brought into the facility will be virus scanned, labeled "unclassified," and initialed by the Security Rep. performing the virus scan. If the media is not to be immediately destroyed a "control" number will be assigned. This media must be stored separately from classified media. More information on unclassified magnetic media can be found in the IS Security General User's Guide (Attachment 4).

a. SAP Accountability. Our classified accountability log book includes the following information:

(1) Document Number

(2) Date Received

(3) Whom the material is From

(4) Document Title

(5) Classification/dia, tri-graph

(6) Disposition to include all transfers or destruction data (date/names of witnesses).

b. SAP Transmission. Classified Material Receipts (CMR) is used to transfer accountable SAP material to other approved facilities. Two copies of the CMR are sent with the material, one for the receiver to keep and one for the receiver to sign, date and return to the CPSO within 30 days. These are retained for five years. No one but the CPSO/ACPSO or PERSEC personnel may transfer classified SAP material out of the Clifton Facility.

Using this process will ensure that accountable material does not leave this facility without Security knowing about it.

c. SAP Reproduction. No classified reproduction is authorized at this time.

5-202. Collateral Material. Collateral classified material required to support a SAP program may be stored within SAPF safes. However there must not be any compromise of program information or any other classified information while Collateral material is being stored in the SAPF. Your CPSO will provide guidance for this material while it's maintained in the SAPF. It can be stored in the drawer with SAP material but in separate folders.

5-203. Annual Inventories.

a. On an annual basis the CPSO and a disinterested party will review the document control and accountability system to ensure the process is operating efficiently and providing effective protection for the program information. This process will include:

(1) 100 percent annual inventory of all Top Secret magnetic media and hard copy documents.

(2) Review of the document control log books.

(3) Review of the disposition/retention process and size of the program holdings.

b. The inventory will begin in September based on the holdings as of that date. This is also an opportunity for us to "clean house."

c. Results of the inventory will be retained for review by the GSSO/PSO during the next scheduled security inspection.

d. When there is a change of CPSO, a 100 percent inventory of all his/her holdings will be conducted.

5-204. Working Papers and Top Secret Engineering Notebooks

a. Working Papers.

(1) If you generate working material (papers) that are not yet in finalized form, and will not be retained longer than **30 days** within the facility, you do not need to enter it into the accountability system. However, you must mark the working papers with the originator's name, portion marking, and "Working Papers" notation and date created/printed in upper right corner of each page and affix a **TS WP coversheet** to the material. We **may not** transmit TS working papers outside the facility by fax or courier. They must be brought into accountability before transmission by the CPSO.

(2) If you have an electronic version of a Top Secret document, you can print a hard copy of it if you insert "Working Papers" and the date printed in your header. This will allow you to utilize the material for a 30-day period as working papers. After that time it must be destroyed or brought into accountability. As long as the Top Secret information is in electronic form, it does not require an accountability number even if it leaves the facility by electronic means.

b. Top Secret Engineering Notebooks.

(1) Top Secret engineering notebooks will be permanently bound documents and pages will not be removed. The Stationary catalog has a supply of hard bound notebooks that can be used for this purpose. Engineering notebooks created prior to May 2008 may be retained for historical reference, but cannot have new information added to them. New bound notebooks must adhere to the following guidelines:

(a) Each notebook must be entered into the Top Secret accountability system by the CPSO or another program briefed Security individual;

(b) The outer cover will be marked with the highest classification to identify the level of information contained in the notebook. A disclosure record coversheet must be used for this purpose;

(b) Each page will be marked with the highest classification (overall classification can be Top Secret) and program identification(s) contained in the overall notebook or on each individual page;

(c) Each page will be numbered consecutively, front and back (i.e., 1 of 50, 2 of 50, etc.). Data incorporated/attached will not be removed;

(d) Portion markings are not required;

(e) Derived From/Declassification instructions are required on the inside cover or first page.

Section 3. Storage and Storage Equipment

5-300. Storage Policy. SAP material must be stored and locked in a GSA-approved safe container. Containers may be left unlocked during normal work hours if the facility is manned and un-cleared visitor procedures are adhered to. An exception to this would be during an emergency evacuation. SCI material that does not contain program information should be stored separately in a safe or drawer. If this isn't possible, it is acceptable to segregate it and store it in the same drawer to enable a non-accessed SCI inspector access to their material without having access to the SAP material. Classified material from other programs cannot be stored in our facility unless a Co-Utilization Agreement (CUA), Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU) or accredation is approved and signed by the PSO and the CSA of the other material. SAP-supporting collateral material can be stored in the program area without a CUA, and may be stored separately within the drawer from SAP and SCI material.

5-301. Control of Locks and Combinations.

a. The CPSO maintains a record of combinations of storage containers and custodians of the containers and/or drawers. Each safe must have a number affixed to the exterior. This number coincides with the number and combination in the safe log. Safe drawers can be numbered 1 through 5 if desired.

b. Combinations must be changed when first installed or used, when believed to have been subject to compromise, when an individual has been removed for cause, or when deemed necessary by the SMC/GPES GSSO. If a container is emptied for removal from the facility, it will first be inspected to ensure no program material is present and the factory setting of 50-25-50 will be set prior to its removal. Inspection will include inspecting behind each drawer.

5-302. Security Container Records of Use. Open/close logs (attachment5) must be completed each time a container is opened/closed. The open/close or open/locked magnetic sign must be turned to the appropriate side. When a safe container log is completed, simply give this form to the CPSO/ACPSO and initiate a new one.

Section 4. Transmission.

5-400. General.

a. The CPSO/ACPSO is responsible for transmission/receipt of all program material leaving/entering the facility with the exception of information sent/received over the Secure Global Network (SGN). **The CPSO and ACPSO are available to transfer material between the hours of 0730-15:00 Monday thru Friday.** Information requiring action after that time will be handled the next business day except in emergency, unavoidable circumstances.

b. The following are approved methods of transmission:

1) Secure Facsimile by means of STEs.

2) Defense Courier Service (DCS) within CONUS.

3) Couriers on commercial aircraft on as required basis with GSSO approval.

4) Classified email – Secure Global Network (SGN)

5) U.S. Postal Service Certified or Express Mail with return receipt – Confidential material only. Secret must be sent USPS Registered or Express Mail with GSSO approval.

6) U/HVSACO and FOUO by First Class Mail.

5-401. Preparation.

a. The CPSO/ACPSO/PERSEC will wrap all packages for transmission outside the facility with the exception of one circumstance: 1) individual is wrapping under the direct supervision of the CPSO/ACPSO/PERSEC. The CPSO/ACPSO/PERSEC will wrap and mark packages as specified below:

(1) Double wrapped with an opaque container (locked briefcase, container or pouch <u>will not</u> act as the second wrap except for local area couriering).

(2) The inner most wrap will be conspicuously marked on all sides with the appropriate classification level (no classified code words). In the center of the package the receiving facility address will be placed and address of sending facility in upper left corner. If appropriate, the package should indicate an addressee (i.e., "To Be Opened Only By: (authorized recipient's name or CPSO)"). In addition to the classification markings, the inner container will be marked with the following on the bottom center of the front:

WARNING!!! IF FOUND, DO NOT ATTEMPT TO OPEN!!!!

> This package contains classified U.S. Government information. Transmission is prohibited by Title 18, U.S. Code, Section 798 (or Title 42, Section XX for RD or FRD Material). If found, please do not open. Please call Tom Oceanak (COLLECT) at (973) 284-3972 or Rosalie Brancatelli at (973) 284-5002 during work hours or (973) 284-3335 after working hours.

(3) Packages hand carried by program personnel will contain the sender and recipient's addresses, sterile addresses if applicable, as well as the package number for tracking purposes. An ITT CMR will be filled out and placed in an envelope in the package.

(4) Material will be wrapped in such a way to provide adequate protection against inadvertent opening/bursting during transit or surreptitious access. Flaps, corners and seams will be fully protected with reinforced tape.

(5) All transfer of program material will require a formal receipting action with the exception of material sent over SGN. Receipts for faxing should be prepared and accompany the material. The CPSO/ACPSO will generate receipts for all transmission of Top Secret material. The receipt must include, as a minimum: control number (if Top Secret accountable), title, overall classification, diagraph/trigraph, number of pages, copy number, sender and recipient. The CPSO maintains a 03 day suspense folder on other locations for return of classified/unclassified material receipts. If receipts are not returned within 30 days, the CPSO/PERSEC/ACPSO initiates a tracer action immediately with a response required within seven days. If the recipient doesn't respond within 15 days to the tracer action, a preliminary inquiry will be initiated immediately and the GSSO/PSO notified.

(6) When classified program material is transmitted within the facility, the material should be placed in an opaque envelope and have the appropriate cover sheets on the document(s).

b. Internal Transfers. Internal movement of Top SECRET SAP material between SAPF's can only be accomplished by the CPSO/ACPSO.

c. Hardware. Prior to any movement of program assets, non COMSEC material, outside the SAPF, you must contact your CPSO/ACPSO for approval. If the Hardware is COMSEC material you must notify the CPSO/CRO/ACRO. This is to ensure a Transportation Plan has been prepared and approved by the GSSO/PSO. Be certain this coordination is accomplished early in the process to avoid delays that could cause schedule slips. 40 days are required for most Transportation plans to be written and approved.

5-402. Couriers.

a. When electronic means are unsuitable for transmission of the material, it may be sent by courier. If you act as a courier, you will read and sign the Courier Instructions (SAP Format 28) and be briefed regarding your responsibilities. For hand carries outside the 50 mile radius, all couriers must also possess a Courier Authorization Letter that our GSSO will approve. GSSO's will only authorize hand carries aboard aircraft when all other means of transmission have been exhausted. Hand carry of Top Secret material requires two persons unless approved in advance by the cognizant PSO.

b. Approval for transmission of Top Secret program material aboard commercial aircraft Must be obtained from the PSO. A single courier can be used for Secret and below materials, but still requires the PSO/GSSO to sign the courier letter. If you courier on commercial aircraft, you must use a lockable briefcase as the third wrap, **no exceptions.** The enclosed locked pouch or wrapped package <u>will not</u> be opened. If airport personnel are persistent, you must terminate your travel and return the classified package to your point of departure. Notify your CPSO immediately. The CPSO will notify the GSSO

c. Approval for OCONUS courier trips must be obtained from AFSPC/A8Z. This authorization is not delegated.

d. The following rules/procedures apply:

1. Before departure, call ahead to your destination to advise them you are departing the Clifton Facility

2. The CPSO will provide you with a list of security contacts for ITT as well as the intended recipient prior to departure.

3. Upon arrival, call back to the CPSO/ACPSO/PERSEC to advise them you arrived.

4. Reverse the procedures when returning if you are couriering classified material.

5. If security at the destination or ITT cannot be reached, call a POC at the applicable location that can relay your departure and/or safe arrival.

6. All materials must come and go through the Security CPSO's at both locations.

7. A cell phone should be carried, if available, in case of an emergency during transit.

g. Individuals briefed to move Secret/SAP hardware between ITT program facilities must always let the CPSO/COMSEC Manager or Alternates know before the move takes place. If the Hardware is visually classified it must be shrouded to prevent inadvertent disclosure.

h. The CPSO needs 35 days to get a transportation plan approved.

i. All incoming packages containing classified program material or equipment must be given to the CPSO/ACPSO for processing before opening. This ensures that transfer receipts are signed for the package contents and returned to the originating facility. Every attempt will be made to process and distribute material within 24 hours of receipt.

5-403. Secure Fax and Electronic Transmission

a. A Secure facsimile may be used for the transmission of SAP Program information when approved in writing by the GSSO. The sending and receiving of secure facsimiles are performed by a briefed program individual.

b. All incoming and outgoing faxes (S or TS) are tracked and logged onto the Fax Log sheets and a tracking number is issued. Fax coversheets must be attached to outgoing faxes and a Document Control number is assigned. The faxing procedures are as follows:

Outgoing FAX Procedure

1. Completely fill out the FAX log sheet and assign the next up FAX number starting with the current year followed by a dash e.g. 11-001. (Attachment 8)
2. Fill out a SAP Form 15 Facsimile Transmission Form to use as the first page of the FAX.
3. Insert proper KSV-21 into the STE and turn on the FAX machine.
4. Dial the distant end FAX telephone number and establish verbal contact.
5. Push the 'Secure Voice' button on the STE. When Secure Voice mode has been established push the scroll button repeatedly until you can validate the distant STE's crypto re-key date is current to within one year. If current, push the 'Secure Data' button. If not current ask the distant end to re-key their STE and re-establish the secure call. Re-check the date.
6. Load the document with SAP Form 15 as the first page into the FAX hopper face down.
7. Push the Start button on the FAX.
8. When the display on the FAX goes back to "Ready", push the Secure Voice button and ask if all of the pages have been received and are legible. If so go to the next step if not, re-fax missing or illegible pages.
9. File the SAP form 15 in the Outgoing FAX folder located in the Safe.

10. Put the faxed document back into the proper folder in the Safe.

Receive FAX Procedure

1. Answer the STE and determine if the distant end wants to FAX a document or have a secure conversation.
2. Whichever the case get the correct KSV-21 from the safe and insert it into the STE.
3. If it is a FAX coming in allow the distant end to initiate the secure sequence. Once in Secure Voice mode push the scroll button repeatedly until you can validate the distant STE's crypto re-key date is current to within one year. If current, push the 'Secure Data' button. If not current, ask the distant end to re-key their STE and re-establish the secure call. Re-check the date.
4. While waiting for the fax to come through, begin to fill in the FAX log sheet and assign the next one up number sequence using the current year then a dash e.g. 11-002.
5. When the coversheet of the incoming fax is ejected into the receive hopper write the FAX number on it.
6. Finish filling out the FAX Log Sheet.
7. After the fax is received attach the proper coversheets to the front and back of the document. Put the received document into the Document control book, close the safe and contact the CPSO/ACPSO. The CPSO or Designate will enter the material into accountability.

5-404. U.S. Postal Services (USPS).

a. ITT Clifton has established a sterile post office box that is not identifiable with the ITT. This box number is not to be given to any organization for the mailing of collateral information to the ITT organization. It is to be used only for SAP program material. No TOP SECRET program material or SCI can be transmitted via the U.S. mail system under any circumstances. CONFIDENTIAL program material may be sent via the U.S. Postal Service Certified Mail (return receipt required) System or U.S. Postal Service Express Mail to the sterile post office box.

(1) This post office box is serviced by the Security personnel at least twice each week. SECRET/SAP material may be sent USPS Registered Mail. USPS Express Mail can be used on a case-by-case basis with approval of the GSSO. Packages may only be shipped on Monday-Thursday to ensure carriers don't retain the classified over a weekend. Note: The "Waiver of Signature and Indemnity" block on Express Mail Label 11-B **may not** be executed and use of external (street side) Express Mail collection boxes is prohibited. No other overnight services are authorized. USPS Certified or Express Mail is authorized for CONFIDENTIAL/SAP material. "For Official Use Only" and Unclassified/HVSACO material may be sent by First Class Mail.

(2) If you require information regarding the sterile post office box, contact the CPSO/ACPSO/PEREC.

Section 5. Disclosure

5-500. Need-to-Know/Release of Information. Information should not be released to program-accessed personnel unless the individual releasing the information has validated the recipient's need-to-know. No program information, unclassified or classified, can be released to any non-program accessed individual, firm, agency, or Government activity without approval from the PSO. All material proposed for public release must be submitted to the PSO 60 days in advance of the proposed release date.

Section 6. Reproduction

a. Classified Reproduction is not authorized at this time.

5-600. Procedures for Top Secret Material.

a. Classified Reproduction is not authorized in any SAPF.

Section 7. Disposition and Retention

5-700. Retention of Classified Material. ITT Contracts personnel must request retention of closed programs through the GPSD/ENS GSSO. Contractors will submit requests for destruction or retention of program material through their CPSO to the Contracting Officer. The Program Manager (PM) will determine retention approval/disapproval for material not required under the FAR. The GSSO will determine requirements for storage and control of materials approved for retention by the contracting officer/program manager,

5-701. Document Reduction. The CPSO/ACPSO will review the classified holdings on an annual basis to reduce the quantity to an absolute minimum. It is also important that you review your soft copy files and delete when no longer required or superseded in order to free up storage space.

5-702. Bids and Proposals. Material received from contractors for white papers, responses to RFPs, etc. must be protected IAW the Company Proprietary requirements identified on the material.

5-703. Methods of Destruction. The Shredder is located in one of the program areas and is approved for destruction of classified material paper, CRYPTO tapes, viewgraphs (transparencies), FD's, CD's and DVD's. Only Program Security is authorized to destroy classified material held in accountability. All non-accountable classified material turned over to Program Security for destruction must have metal fasteners, binder clips, etc. removed. Also remove staples and paper clips prior to shredding in the program area containing the shredder. The metal destroys the shredder blades resulting in a costly repair and non-compliant shred residue size.

5-704. Destruction Procedures. Material designated for mass destruction, with the exception of magnetic media, will be destroyed at least once a week.

a. All classified and unclassified paper material (i.e., notes, memos, phone messages, phone lists, recall rosters, travel itineraries, copier/printer errors, etc.) will be shredded. The "holes" from punches must also be destroyed as classified waste. Waste cans located in each office will be checked for paper before you place them in the hall for pickup by the janitors. If you have a reason to deviate from these procedures, notify the CPSO for further guidance. Your area wastebasket should contain only lunch residue, disposable coffee cups, dirty tissues, outside wrap from paper reams, etc.

b. Program Security personnel will complete Certificates of Destruction for Top Secret accountable material. Two individuals, cleared to the level of the material, will accomplish and witness the destruction. The certificates will include, as a minimum, control number, title, number of pages, copy numbers, date of destruction and signature of the two destruction officials. The destruction certificate will be maintained for five years.

Section 8. Construction and Other Security Requirements

5-800. General. No program information may be discussed, stored or processed in a facility until it has been approved/accredited for that purpose. This means that it meets the physical security requirements established for SCI/SAP facilities.

5-801. Physical Security. The integrity of the facility must be maintained requiring all proposed modifications be submitted to the GSSO/PSO for review and approval.

5-802. SAPF's Identification. All SAP facilities are assigned a facility identification number to be used in lieu of the company name on receipts, visit certifications, etc. The facility identifier for ITT Clifton program areas is 640-14.

5-803. Prohibited Items.

a. Electronic equipment poses an inherent vulnerability and must be controlled. ITT Clifton personnel are solely responsible for knowing the technology associated with their devices. Portable Electronic Device (PED) is used to describe a wide-range of readily available, small electronic devices such as Palm Pilots®, Blackberries®, Handspring® devices or similar personnel data assistants (PDAs), data diaries, palmtop, laptop, and other portable computing devices. In addition to these devices, the following items are also prohibited in the SAP.

(1) Two-way transmitting equipment including intrabase/land mobile radios in non-emergency situations.

(2) Cellular telephones or any device with radio frequency (RF) capability.

(3) Devices with camera/imaging capability.

(4) Devices with audio/video/data recording and playback features.

(5) Devices with a microphone.

(6) Watches and other devices with communications or synchronization software/hardware.

(7) Cameras and film, unless specifically approved by the PSO for a mission requirement.

(8) iPods, personal organizers etc.

b. The following items are authorized with CPSO approval:

(1) Electronic calculators, spell checkers, language translators, etc.

(2) Receive-only pagers.

(3) Infrared (IR) devices that convey no intelligence data (text, audio, video, etc.) such as IR mouse and/or remote controls.

c. Mission essential government/contractor-owned laptops introduced into the facility will be approved by the IAM and conform to the requirements outlined in the Systems Security Plan on a case by case basis.

d. If there is any doubt as to whether a device is prohibited, contact the CPSO or ACPSO prior to bringing it into the facility. Any waivers to the policy shall be in writing and approved by the GSSO/PSO.

5-804. Magnetic Media.

a. Prior to introducing unclassified magnetic media in to the SAPF, the magnetic media must be taken immediately to Security for virus scanning prior to being loaded onto any SAP computer system. This will be accomplished on dedicated stand-alone machines located in the security department with the most current Antivirus software. Media is scanned for viruses and executables along with level of content. If classified magnetic media is received the CPSO will notify the IAM or IAO before allowing the material to be introduced to a SAP computer.

b. All software/media will be brought into accountability IAW the JAFAN 6/0 Section 8-102 or removed from the facility immediately upon completion of the installation if READ ONLY feature is tested and passes. If the test fails, software cannot be removed from the SAPF and will either be controlled or destroyed.

c. ITT Clifton Information Assurance Officer (IAO) handles all software programs, operating software, and any disk with an **.exe** file. The Information Assurance Manager (IAM) will approve all changes to the software list.

The following are examples of acceptable software:

(1) Provided officially by another U.S. Government agency with equivalent standards.
(2) Provided under contract to organizations involved with the processing of SCI and related intelligence information.

(3) Developed within a Government-approved facility.
(4) Provided through appropriate procurement channels, i.e. COTS software.
(5) Distributed through official channels.
(6) Acquired from a reputable vendor for official use or evaluation (i.e. maintenance diagnostic software).

d. The following software is prohibited:

(1) Games
(2) Public domain software or "shareware" which was obtained from unofficial channels.
(3) Software applications that have been developed outside Government-approved facilities such as those developed on personally-owned computers at home or software acquired via non-U.S. Government "bulletin boards."
(4) Personally-owned software (either purchased or gratuitously acquired).
(5) Software purchased using employee funds (i.e. from an activity such as a coffee fund).
(6) Software from unknown sources.
(7) Illegally copied software in violation of copyright laws.

5-805 Access Control and Alarm Systems. Access to the program areas are controlled by an automated access control device. The ITT Clifton main gate guard Control Station at 77 River Road has a list of individuals to be called, in descending order, should a problem arise in either SAPF. Only individuals on the CPSO approved open/close list are able to open and close. See section 5-109 for specific open and close procedures.

- **SAPF's 287, 241, 242, 004, 042**
- For entry into these SAPF's we utilize Kaba Mas X09 locks, UL approved ADT IDS and Securetron DK2FSF digital entry Ciphers.

- **SAPF 021,020**
- For entry into these areas we use Kaba Mas X09 locks, UL approved alarm systems and ADT card access readers which the user swipes their badge and enters their unique pin to enter the facility.

5-806. Security Checks and Inspections.

a. Our SAP facility entrance doors are not monitored by 24 hour guards or other personnel. Therefore, we must conduct random searches of all hand carried items. These items include personal organizers, lunch and gym bags, purses, briefcases, etc. These searches are conducted randomly Program Security personnel on entry and exit of the all SAPF's. These search records are maintained in program security and are available to the GSSO upon request. These searches are conducted to guard against the introduction of contraband, unauthorized software, portable storage devices, unauthorized electronic devices, and illegal removal of program material.

b. Closing Procedures. A clean desk policy is enforced to preclude individuals from leaving classified material on their desk while out of the office within the program area. Items listed on the end-of-day checklist located at the main entrance of both SAPF's should be thoroughly reviewed prior to checking the item or placing your initials beside it. GPSD/ENS should update the list as necessary. Safe checks must be recorded on the Safe open/close record. Each container must be checked at day's end, even if the custodian has not been present, to verify it was not opened.

(1) When closing the SAPF for the day, follow these procedures:

(a) The last person leaving either SAPF must review the checklist and ensure that all items have been checked. Remember, initialing the checked column on the door open/close sheet is acknowledgment that ALL checks have been completed in accordance with this SOP. This list should include, but is not limited to:

- Individual desks, tables, bookcases, etc. are free of classified.
- Classified waste containers are empty.
- Each safe is locked.
- All STE cards removed and stored in safe.
- Whiteboards clean or contain NO CLASSIFIED (information marked as (U)).
- IS equipment secured (disks, drives (if required), etc.).
- Electric items turned off (copiers, printers, coffee makers, fans, CD players, etc.).

(b) The individual then flips the open/close sign on the exterior of the SAPF main entrance to "CLOSED".

(2) Any deviation and/or irregularities noted during the completion of the end-of-day security checklist will be brought to the attention of your CPSO as soon as possible at the beginning of the next duty day. Any major problems or potential security incidents will be brought to the attention of the CPSO immediately. It is the responsibility of every individual to report any potential or actual security discrepancy no matter how seemingly minor.

5-807. Equipment/Furniture Removal.

a. Prior to removal of any equipment (copiers, computers, etc.), furniture or safes from the SAPF, the equipment must be inspected to ensure no classified information is contained within. These devices will only be sanitized for removal by the IAO or IAM and approved by the GSSO. Each device will be inspected to ensure that all non-volatile memory components are removed before being taken outside the SAPF. Sanitization Forms which can be found in the General User Guide (Attachment 4) and the current SSP will be used. Inspections also include a complete review of interior areas of the furniture, equipment or safes. Safes must be reset to the factory setting (50-25-50) prior to removal if emptied. Computer equipment, peripheral devices, copiers, etc. cannot be removed from the facility until the Hardware Sanitization and Release Record form has been completed and signed off.

b. Equipment or furniture removal needs be coordinated in advance by contacting a ITT Clifton program security representative or the IAM/IAO. Sufficient time should be allowed to accomplish this coordination effort. Only program security personnel and/or the IAM/IAO can remove/introduce equipment.

CHAPTER 6

VISITS AND MEETINGS

Section 1. Visits

6-100. General. A written visit notification will be coordinated in advance of visiting a program area. All SAP visits will be coordinated and transmitted by the CPSO/ACPSO or PERSEC. SCI visits will be coordinated and transmitted by program CPSO/ACPSO or PERSEC. Collateral visits will be accomplished by the contractor FSO.

6-101. Outgoing SAP Visits. If you plan to visit another program facility, you must provide that location a visit notice at least three working days prior to the date of the visit. ***Contact the CPSO/.ACPSO or PERSEC to prepare the SAP visit notice for transmission***. Attachment 3 is an example of the information you must provide to them to prepare the visit notice. The visit notice, accompanied by proper ID (Driver's License), satisfies the "third party" requirement in situations where you've never met your point of contact. Visits must be sent via SGN or fax using SAP Format 7. ***You cannot certify your own visit.***

a. In most cases your SI/TK (SCI) accesses are included with your program access(s). If you travel to a facility where your SCI must be used outside the program area for entry, unescorted access, etc., your SCI must be sent through SMC/IN (SSO) channels. Military and DoD civilian requests must be made through GPSD/ENS.

b. Government and military personnel: N/A

c. Contractor employees must contact their company security representative to send collateral or SCI visits through JPAS.

d. If you are required to sign in at a central lobby in a facility, check the "No" box under the heading "Classified Visit" if applicable. Your clearance information is included on your SAP program visit notification via SAP channels only. If the location requires your collateral to be sent for access, you must coordinate this with ITT Clifton security or FSO. Your CPSO should be consulted for specific information before any visit.

6-102. Identification and Control of Visitors

a. Incoming Accessed Visitors. All visitors without access to the ITT Clifton Facility must enter through the front lobby area. Have the visitor call you from the lobby when they arrive. A visitor is anyone not directly assigned to the Clifton Facility. Individuals from other ITT facilities that have their own ITT badges are not required to sign the Front Lobby Visitor Log. **Accessed outside contractor personnel, other than those residents in the**

facility, are issued “Escort required” badges. If “No Escort Required” badges are required, Program security personnel must authorize them. The lobby receptionist has a list of those authorized for “Non Escort Required” badges.

(1) After your visitor has called from the lobby, you must go to the lobby and show your ID badge to the lobby receptionist.

(2) You are responsible for monitoring the person(s) that you escort into the program area and verifying their visit has been received with the CPSO. You must know their clearance/access(s) before conveying any classified information. You must ensure that visitors do not have in their possession any of the controlled or prohibited items listed in Sections 5-803 or other sensitive data.

(3) When escorting an accessed visitor, have them complete the "Program Briefed Visitor Log". Be certain they complete all entries and enter the time they depart the facility. You must also sign as the escort.

(4) If the visitor is not accessed to all programs, you must activate the red light, and make others aware of their presence before escorting the individual into the SAPF. The SAPF will be sanitized of any visually classified information the visitor is not accessed to. Persons occupying the area must close their doors and be cognizant of their discussions until the visitor departs.

b. Incoming "Non-Accessed" (Un-cleared) Visitors. Individuals without program access are considered non-accessed visitors. Non-accessed visitors should be kept to a minimum unless their services (janitorial/maintenance/photographer) are required. This will provide for the least amount of disruption to program activities.

(1) All non-accessed visitors must complete the “Non-Briefed Visitor Log”. The escort must also enter their name on the log. They must be closely escorted at all times. ***Individuals being escorted for their initial indoctrination briefing must sign the non-accessed visitor log.*** You may only escort as many non-accessed visitors as you can keep under constant surveillance.

(2) You must notify all personnel in an area that a non-accessed visitor(s) will be in the area **BEFORE** you escort them in. Complete this action before you pick them up in the lobby. Take the visitor only to the areas that have been cleared of classified material.

(3) Flashing red light must be turned on when a non-accessed visitor(s) enters your area and will remain on until the visitor has departed. Persons occupying the area must close their doors and be cognizant of their discussions until the visitor departs.

(4) **Do not discuss classified information or leave safe drawers open while non-accessed visitors are in your area. Voices carry easily from one office to another. In addition, protect or cease copying, processing or printing of classified material.**

c. All visits to subcontractors by other subcontractors will be processed through the prime contractor. Visit notification between contractors with no contractual relationship will be approved by GPSD GSSO or his designated representative to certify "need-to-know." The ITT CPSO cannot approve these visits.

Section 2. Meetings

6-200. General. Program classified discussions or meetings must only be conducted in accredited facilities.

6-201. Host Responsibility.

a. For larger meetings an individual should be appointed to ensure adequate security is provided for the meeting. Visitors will need to sign in and be escorted from the lobby. Meeting monitors or hosts are responsible for:

(1) Maintaining an access list, ensuring visit requests are received, checking personal IDs, and controlling access to the room.

(2) Establishing the access level of the meeting or separate portions of the meeting/briefing.

(3) Safeguarding and controlling notes, presentation materials, etc.

(4) Informing attendees and presenters of security limitations, highest classification level, access levels and "must know" requirements for the attendees.

(5) Providing adequate and approved storage capability and ensuring classified materials are transmitted to the attendee's locations.

b. Hosts of meetings can provide attendees with blank classified meeting notes. They are available from the CPSO. These blank classified meeting notes include a cover sheet, blank headers and footers, and working papers notation in upper right hand corner. If the attendees want their meeting notes returned to their facility by fax or courier, they must first be brought into accountability before they're transmitted.

c. Hosts of the meeting and/or presenters must provide sufficient classification guidance to enable the attendees to identify the classification level of the information presented. This information can be provided orally and with appropriate classification markings on audio and visual products.

d. Meetings

a. Post a sign on the conference room door, example below, prohibiting unauthorized personnel from entering while the meeting is in progress.

STOP
DO NOT ENTER.

CLASSIFIED MEETING IN PROGRESS.
KNOCK FIRST AND WAIT FOR THE
DOOR TO BE ANSWERED

DO NOT ENTER.

b. Once the meeting has concluded, the conference room must be checked to verify all classified material has been removed.

CHAPTER 7

CONTRACTING

Section 1. General

7-100. General.

a. Program contracting will establish legal obligations in such a manner to prevent unauthorized personnel from becoming aware of the actual source of funding, program activity relationships, and methods and techniques used to execute and administer the unacknowledged contracts.

b. The Defense Security Services is carved out from cognizance over our SAP programs depending upon the classification or protection requirements for that specific program.

7-101. Procedures.

a. Initial Contact. Any initial contact between ITT program personnel and a potential program contractor will be made through the GPSD Contracting Officer. He/she will ensure proper Organizational Conflict of Interest (OCI) by insuring these initial contacts do not reveal program information or relationships, if applicable.

b. Sub-Contractor Selection. The CPSO will play a major role in any contractor selection process. The GSSO's evaluation of a contractor's security capabilities will be a major factor in the selection process right along with the contractor's technical capabilities.

(1) When contractors require subcontractors or vendors not accessed to the program, they must complete and forward to the GSSO for approval a Subcontractor/Supplier Data Sheet (SAP Format 13). No contact will be made until the request has been formally approved.

7-102. Contract Security Classification Specifications (DD Form 254).

Each GPSD/ENS prime contractor must be issued a DD Form 254 that identifies to the contractor specific and comprehensive guidance on procedural and classification specifications. DD254s for some programs are classified at the program level and maintained within program channels. Acknowledged SAP or collateral DD254s can be maintained outside program channels. Prime contractors will develop DD254s for all subcontractors who participate in program aspects of the program and will be approved by the appropriate GSSO prior to submission to the subcontractor.

7-103. Security Oversight. The GSSO/CPSO will exercise full security oversight over the sub-contractors to include security review responsibility.

CHAPTER 8

INFORMATION SYSTEMS (IS)

Section 1. General

8-100. General.

a. Information Systems (IS) is a generic term applied to an electronic computing system. These systems are composed of computer hardware (e.g., automated data processing equipment (ADPE) and associated devices which may include communication equipment), firmware, operating systems, applications and other applicable software. Information Systems collect, store, process, create, disseminate, communicate and/or control data or information.

b. The ITT Clifton Information Systems (IS) Security General User's Guide is Attachment 4 to this SOP. Questions regarding IS should be addressed to the ITT Clifton Information Assurance Officer (IAO) or Information Assurance Manager (IAM). The IAO/IAM and his/her staff are responsible for implementing and monitoring all IS security functions. The IAO and IAM are located in the Clifton Facility. The IAO is responsible for all hardware and software installation, troubleshooting, etc. The IAO can be reached at 973-284-4060, IAM on x4237.

CHAPTER 9

MISCELLANEOUS

Section 1. Document Retention

9-100. General. Program documents will be retained according to the schedule shown below:

Document Retention Schedule

Type of Document	**Retention Period**	**OPR**
Visitor Logs	5 years	CPSO
Visit Notifications/Requests	1 year	CPSO
Document Inventory Reports	After PSO/GSSO/CPSO Review	CPSO
Data Transfer Receipts (Facsimile & Courier)	5 years	CPSO
Mail Receipts/Logs	2 years	CPSO
Top Secret Access Records	2 years after material is destroyed	CPSO
Destruction Certificates	5 years	CPSO
Security Inspection Reports	After PSO/GSSO/CPSO Review	CPSO
Entry/Exit Random Checks	After PSO/GSSO/CPSO Review	CPSO
Safe Check Records	After PSO/GSSO/CPSO Review	CPSO
Door Open/Close Logs	After PSO/GSSO/CPSO Review	CPSO
Security Violations/Infractions	5 years after program termination	CPSO
Security Classification Guides	Retain permanently	CPSO

Section 2. Operations Security (OPSEC)

9-200. General.

a. Operations Security (OPSEC) is a process that identifies and protects critical information concerning intentions, capabilities and current activities. This information is comprised of unclassified indicators. The methodology identifies critical information for risk management. OPSEC is a process to deny potential adversaries information about capabilities, and/or intentions by identifying evidence of the planning and execution of sensitive activities. The OPSEC process consists of five steps:

(1) Identification of critical information,

(2) Analysis of threat,

(3) Analysis of vulnerabilities,

(4) Assessment of risks, and

(5) Application of countermeasures.

b. The goal of OPSEC is to make hostile intelligence gathering more difficult and time consuming. The longer it takes for an adversary to acquire our national secrets, the longer our nation can maintain its military and technological edge.

c. All accessed personnel are responsible for understanding the OPSEC concept and the foreign intelligence threat to program operations. The ITT Clifton OPSEC Plan is located in the Program Security Binders located in the 287 room. Contact the CPSO for access to the OPSEC plan

9-201. Responsibilities and Management.

a. The Contractor Program Manager(s) are responsible for ensuring that OPSEC is fully integrated into all phases of the acquisition process.

b. The Facility Security Manager is designated as the OPSEC Program Coordinator. He provides OPSEC policy, guidance and direction to all Clifton personnel. He is responsible for conducting an annual review and evaluation of the OPSEC program to determine its effectiveness in the preceding year and to develop recommendations for improvements for the coming year and the longer term. Initial OPSEC training is conducted during the initial program indoctrination briefing. OPSEC will be included in the Annual Refresher training. Recurring training is conducted as information is received or developed to maintain a heightened sense of OPSEC awareness.

c. The ITT OPSEC Plan provides guidance for ITT employees and other contractor personnel involved in ITT activities concerning the protection of classified and unclassified information, and sensitive operations and activities that could potentially reveal classified information to individuals with no need to know.

d. Paper has been shredded properly.

e. Be aware of your surroundings when discussing SAP information. Classified information should never be discussed outside an approved SAP facility, but unclassified, sensitive information can also indicate program intentions. Always be alert to your environment and who might be listening to your conversation.

Section 3. Emergencies

9-300. General. All personnel should have ITT emergency number x4444 posted next to their phone. If you do not have one, contact a security representative. Any threats should be reported to ITT security @ 973-284-4480.

9-301. Protection of Classified During Emergencies. In most cases, there is ample time to follow some basic security practices when evacuating the area during an emergency. Check the area for anything that should be secured and store it in a safe and lock the container and logoff and power down computers if time allows. **Classified material will not be removed from the area during an evacuation. Refer to the Emergency Action Plan (EAP).**

9-302. Access by Emergency Response Personnel. Emergency response personnel will be given unrestricted access to each room of the area in order to perform their duties by the first individual contacted by them. Do not restrict their access and do not place yourself in a dangerous situation. Security representatives will handle the follow-up process required for emergency personnel after the emergency is over.

9-303. After Hours Emergency Access. ITT Security Officers will contact the CPSO/ACPSO/FSO to respond to the SAPF via the Emergency Access List provided for each SAPF. Program Security will open the area and escort the individual(s) at all times.

9-304. IDS/ALARM Testing. The SAPF alarms will be tested semi-annually to ensure they are in good working order. The response time, the activation time and responder will be noted in the Alarm Log Sheet and filed in the security binders. (Attachment 6)

9-305. Entry/Exit Inspections. Entry and exit inspections will be conducted by the CPSO/ACPSO periodically but no less than once a month. All material (i.e. folders, papers, backpacks, briefcases etc.) will be inspected for content. Material not directly related to the program will be removed immediately. (Attachment 7)

Program Security Support

Mark S. Fallon
IEWS Manager
Security

284-4480

Richard Zymroz
IAM
SecurityComputer

284-4537

Thomas Oceanak
Contractor Program
Security Officer/SFO

284-3972

Michael Rusciano
Personnel security
A/CRO

284-5450

Rosalie Brancatelli
AI Contractor
Program security
Officer

284-5002

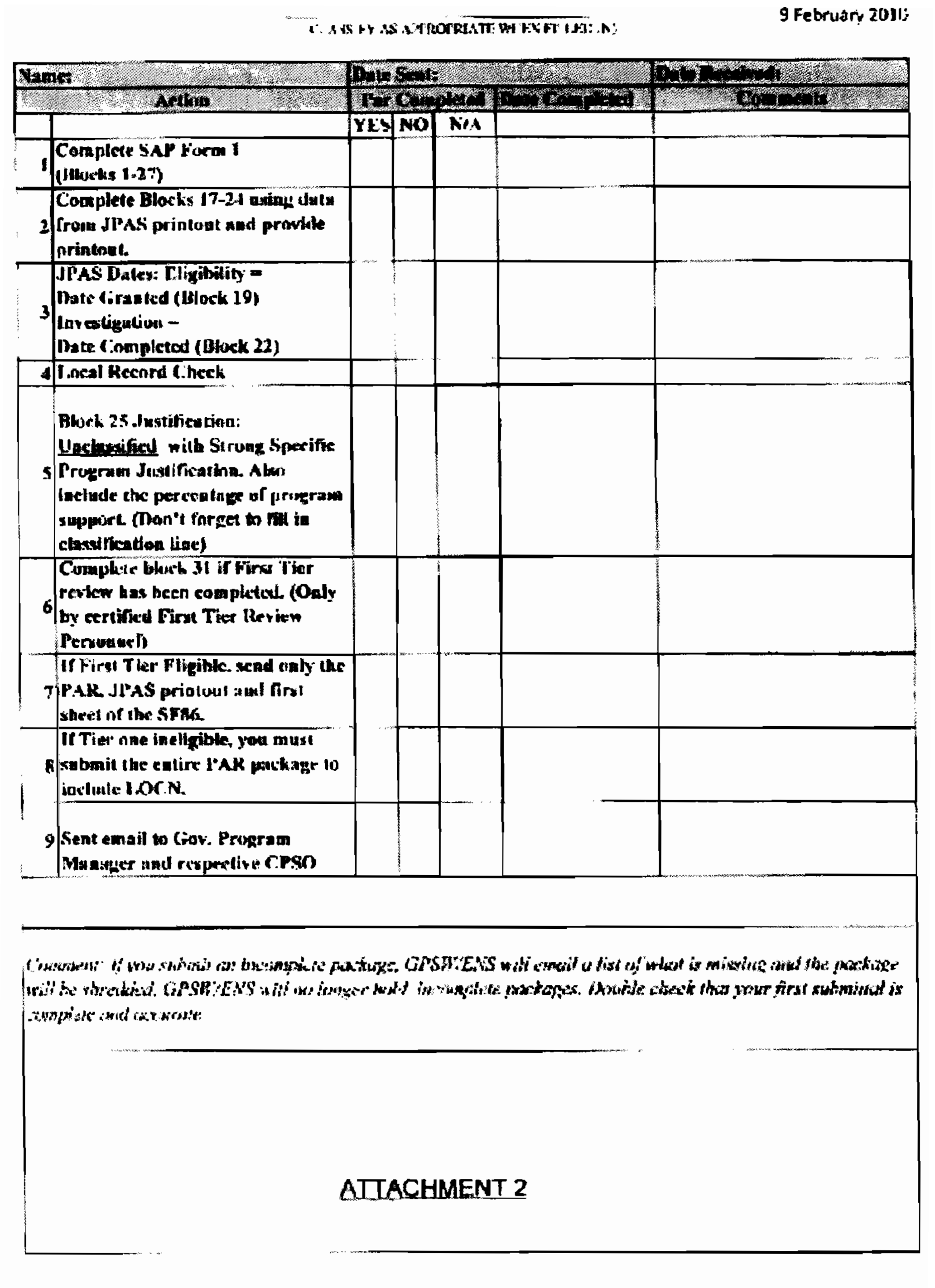
Joe Calabro
IAO
Computer Security

284-4060

Karen DelMauro
PERSEC

284-3255

ATTACHMENT 1



(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

9 February 2010

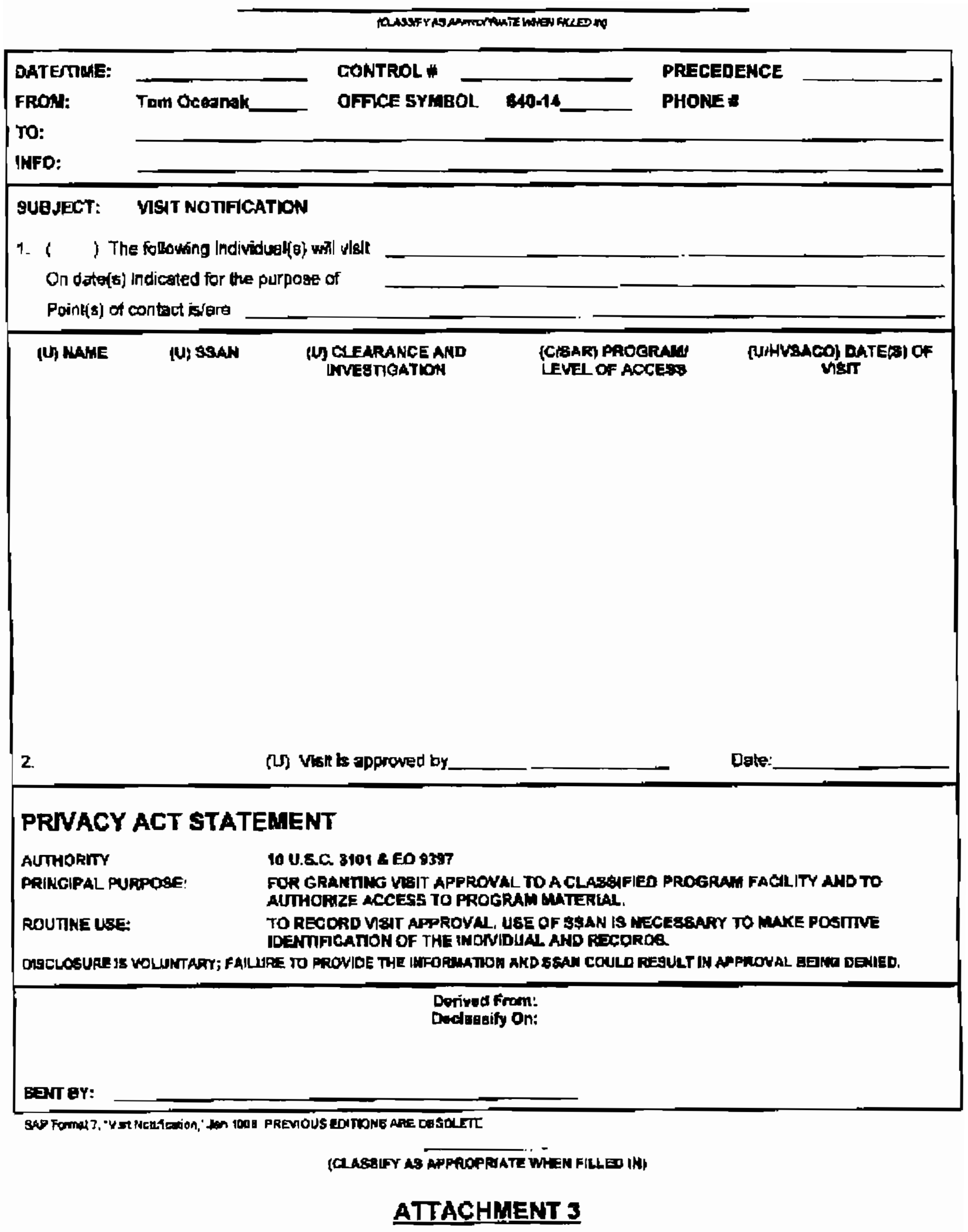
Name:		Date Sent:				Date Received:
	Action	For Completed			Date Completed	Comments
		YES	NO	N/A		
1	Complete SAP Form 1 (Blocks 1-27)					
2	Complete Blocks 17-24 using data from JPAS printout and provide printout.					
3	JPAS Dates: Eligibility = Date Granted (Block 19) Investigation – Date Completed (Block 22)					
4	Local Record Check					
5	Block 25 Justification: <u>Unclassified</u> with Strong Specific Program Justification. Also include the percentage of program support. (Don't forget to fill in classification line)					
6	Complete block 31 if First Tier review has been completed. (Only by certified First Tier Review Personnel)					
7	If First Tier Eligible, send only the PAR, JPAS printout and first sheet of the SF86.					
8	If Tier one ineligible, you must submit the entire PAR package to include LOCN.					
9	Sent email to Gov. Program Manager and respective CPSO					

Comment: If you submit an incomplete package, GPSW/ENS will email a list of what is missing and the package will be shredded. GPSW/ENS will no longer hold incomplete packages. Double check that your first submittal is complete and accurate

ATTACHMENT 2

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

ATTACHMENT 2



(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

DATE/TIME:	______	CONTROL #	______	PRECEDENCE	______
FROM:	Tom Oceanak______	OFFICE SYMBOL	840-14______	PHONE #	
TO:	______				
INFO:	______				

SUBJECT: VISIT NOTIFICATION

1. ( ) The following individual(s) will visit ______

On date(s) indicated for the purpose of ______

Point(s) of contact is/are ______

(U) NAME	(U) SSAN	(U) CLEARANCE AND INVESTIGATION	(C/SAR) PROGRAM/ LEVEL OF ACCESS	(U/HVSACO) DATE(S) OF VISIT

2. (U) Visit is approved by______ Date:______

PRIVACY ACT STATEMENT

AUTHORITY	10 U.S.C. 3101 & EO 9397
PRINCIPAL PURPOSE:	FOR GRANTING VISIT APPROVAL TO A CLASSIFIED PROGRAM FACILITY AND TO AUTHORIZE ACCESS TO PROGRAM MATERIAL.
ROUTINE USE:	TO RECORD VISIT APPROVAL. USE OF SSAN IS NECESSARY TO MAKE POSITIVE IDENTIFICATION OF THE INDIVIDUAL AND RECORDS.

DISCLOSURE IS VOLUNTARY; FAILURE TO PROVIDE THE INFORMATION AND SSAN COULD RESULT IN APPROVAL BEING DENIED.

Derived From:
Declassify On:

SENT BY: ______

SAP Format 7, "Visit Notification," Jan 1998 PREVIOUS EDITIONS ARE OBSOLETE

(CLASSIFY AS APPROPRIATE WHEN FILLED IN)

ATTACHMENT 3

ATTACHMENT 3

“ITT Corporation”

General User’s Guide for Z09-004, Z09-042, & Z-241

ATTACHMENT 4

Version: 1.0.0
September 23, 2010

Revisions

Date	Revision	Page	Description of Change

Table of Contents

1.0 LAN/Workgroup Overview

The LAN/Workgroup is used to perform administrative and engineering document and program development in support of SAP/SAR information system (IS) requirements.

The LAN/Workgroup is made up of PL2 computers that which employs unique security features approved by the DAA. A PL2 computer means that all users have Formal Access Approvals, but NOT ALL Users Have a Need To Know for ALL the Information on the computer.

2.0 Points of Contact

Contractor Program Security Officer (CSSO): Tom Oceanak, 973-284-3972

Information Assurance Manager (ISSM): Richard Zymroz, 973-284-4237

Information Assurance Officer (ISSO): Joe Calabro, 973-284-4060

System Administrator (SA): Contact the ISSM or ISSO for specific System Administrator (SA) names and phone numbers.

3.0 Account Application Process

Computer accounts are requested by the Program Manager or CSSO to the ISSM. The ISSM will make final determination for creating the account.

When the account is authorized, the ISSO or ISSM will provide training for the new user, the new user will read the General User's Guide, and sign the Computer System User Acknowledgement Statement. This form is given to the SA, ISSO or ISSM for account creation.

4.0 Training Requirements

New users receive AIS training from the ISSO or ISSM prior to receiving a user account. The training contains the minimum information required to meet security policy.

Annual refresher training is provided by the CSSO, ISSO, or ISSM every year. This training is mandatory and failure to attend will result in the user's account being disabled.

5.0 Password Policy

Passwords must be at least 8 characters long with complexity that consists of upper and lower case letters, numbers and special characters. For example ABC!abc1 is a valid password.

Passwords expire every 90 days. You can not use a previous password going back 24 passwords. Do not use a word or name in the password to include variations injecting special characters (C@T).

Passwords will not be written down. Users will not share their user ID and/or password with any other individual.

6.0 Resetting Passwords

After three failed logon attempts a user's account will be locked out.

If a user account is locked as a result of three failed logon attempts, the user must contact the SA, ISSO, or ISSM. The SA, ISSO, or ISSM will verify the user's identity and re-enable the user account.

7.0 User Acknowledgement

All users will read this agreement prior to receiving an account:

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.
- You consent to the following conditions:
  - The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
  - At any time, the U.S. Government may inspect and seize data stored on this information system.
  - Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
  - This information system includes security measures (e.g., authentication and access controls) to protect U.S. government interests--not for your personal benefit or privacy.
  - Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
    - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

    - The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

    - Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

    - Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

    - A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

    - These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

- In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

- All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

I understand that as a computer system user, it is my responsibility to comply with all security measures necessary to prevent unauthorized disclosure, modification, or destruction of information. Signature on this sheet indicates MY understanding and acknowledgement of the rules detailed below. Use of these computer systems is a privilege. Failure to comply with all rules and regulations pertaining to the use of the computer systems CONSITUTES A SECURITY INCIDENT and will result in the loss of privileges.

I will protect and safeguard information in accordance with (IAW) the established procedures and will sign all logs forms and receipts as required.

Escort personnel not on the access list for the environment in such a manner as to prevent their access to data that they are not entitled to view. Notify personnel on clearance level of visitor(s) prior to granting access within program areas.

Protect all media used on the system by properly classifying, labeling, controlling, transmitting and destroying it in accordance with security requirements. All media and hardware will be brought into accountability.

Protect all data viewed on the screens and/or hard copies at the highest classification level of the data processed unless determined otherwise by the data owner, and bring into accountability.

Immediately notify the ISSO/ISSM of all security violations, unauthorized use, and when I no longer have a need to access the system (i.e., transfer, termination, leave of absence, or for any period of extended non-use).

Use of the system is for the purpose of performing assigned organizational duties, never personal business and I will not introduce process, calculate, or compute data on these systems except as authorized according to these procedures.

I will not add/remove/or modify any system hardware or software without written authorization from the ISSM, and will not violate any software copyright laws and licensing agreements.

Never allow anyone to use my login ID and Password, or write the Password down.

I will utilize the Screen Saver application with a maximum of fifteen minutes for activation and password protected.

I will save any data to the appropriate COMMON PROJECT FOLDER and will not save any data to my "C" drive or Desktop. The COMMON PROJECT FOLDER is the only place that information can be saved to. Permission must be obtained from the ISSO or ISSM prior to saving any information to removable media drives (i.e., floppy/CDROM).

I will never transfer information from these computer systems to any non- program systems.

I understand that I am subject to monitoring at all times while using these systems.

8.0 Physical Protection Standards

These systems are physically protected by the facilities that house it. Security in depth is incorporated to include and not limited to locks, alarms, access lists and technical security features.

Screensavers are set to 15 minutes of inactivity. However, users are encouraged to always lock the screen when they leave the computer. Using [cntrl] [alt] & [del] than [enter] or the [windows] [L] will lock the screen.

9.0 System Startup/Shutdown Procedures

These workstations should only be used during normal hours of operation, which are from 7:00 AM to 7:00 PM Monday through Friday. The PC's will always be powered down with their removable disk drives locked in an approved Program security container when the PC's are not in use.

Exceptions to the hours of operation may be made in advance through the CSSO or the ISSM.

Each accredited PC shall has an internal fixed disk so there are no special startup/shutdown procedures.

10.0 Media Introduction

All media entering the Program Area must be have a Request to Install Software/Data form filled out. The media and Request to Install Software/Data form will be handed over to the ISSM, ISSO, or Program Security.

The ISSM, ISSO, CSSO, or the Security Administrator shall check the media for virus and malicious code.

The ISSO or ISSM or SA will copy the files from the media to the systems.

The ISSM, ISSO, CSSO, or the Security Administrator will then enter the media into program accountability and store the media in approved storage containers.

11.0 File Transfer Policy

Low to High transfer is defined as moving data from a lower classification system to a higher classification system and will to be requested via email to the ISSO or ISSM. It must have the ISSO or ISSM approval prior to being performed.

High to Low (higher classification system to a lower classification system) transfers not normally allowed. However if the higher classification system to a lower classification system is mission critical a request will be sent to the government Program Security Officer for review and approval. Prior approval by the PSO must be obtained before the higher classification system to a lower classification system transfer is allowed. The preferred method of transferring data to lower level IS is by use of a scanning software. Security review of a document being scanned is also required. The individual scanning the document is responsible for any spillage resulting from the scan.

12.0 File Plan and Policy

Each user will store all data on the COMMON PROJECT FOLDER. No data is to be stored anywhere else.

13.0 File Recovery

The SA will backup files from the COMMON PROJECT FOLDER on a weekly basis. Backups allow them to go back up to three months to recover data. In the event of lost data, contact the SA for assistants.

14.0 Incident Reporting

In the case of a suspected or actual AIS incident, report your concerns to the ISSO and the ISSM immediately.

The ISSM, ISSO or CSSO as appropriate, must report all abnormal security events to the DAA. Incident reporting shall be accomplished by through the ISSM, ISSO or security channel, such as the CSSO.

15.0 Software Request Procedures

All requests for additional software will be submitted to the ISSM.

Foreign software, freeware, shareware and home grown software are not authorized without DAA approval

16.0 Hardware Request Procedures

All requests for additional or replacement hardware will be submitted to the ISSM.

Additional security concerns may exists and final approval for hardware may require further security approval.

ATTACHMENT 5

SAFE, CABINET, OR CLOSED AREA SECURITY RECORD

SAFE OR CABINET IDENTIFICATION Entrance to 241 SCIF:

PHYSICAL LOCATION Pole Location R-43
Clifton NJ

SECURITY AREA SCIF LAB

YEAR:

DOUBLE CHECK AREA NUMBER 241

AS INDICATED BY MY INITIALS BELOW I HAVE UNLOCKED, LOCKED, OR CHECKED THE ABOVE IDENTIFIED CONTAINER ON DATE AND TIME NOTED. IN LOCKING OR CHECKING THIS CONTAINER I HAVE ASCERTAINED THAT ALL DRAWERS (OR DOORS) HAVE BEEN CLOSED AND, WHEN APPLICABLE, THAT THE LOCKING BUTTON IS IN THE LOCKED POSITION; AND THAT I HAVE ROTATED THE DIAL AT LEAST FOUR TIMES IN THE SAME DIRECTION.

	Unlocked By		Locked By		Checked By	
Date	Time	Inital	Time	Inital	Time	Inital

	Unlocked By		Locked By		Checked By	
Date	Time	Inital	Time	Inital	Time	Inital

ATTACHMENT 6

Special Program Areas Alarm Log/Guard Response

Date____________

Test conducted for following areas:____________________

Time alarm was set off: ____________________________

Time alarm was responded to: _______________________

Who responded: __________________________________

Results: ____

Name of individual conducting the test: ________________________________

Signature:____________________________

ATTACHMENT 7

SAP ENTRY / EXIT INSPECTION LOG

Date of Inspection	Z or NZ #/Location	Time of Inspection	Individual Inspected	Findings/ Results	Official conducting inspection

FAX LOG SHEET

Date	Time	Fax No.	From	To	Class	No. of Pgs	Forward To	Unclassified Title	Station Operator

ATTACHMENT 8