

CHANGE**U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION****ORDER 1600.76
CHG 1**

National Policy

Effective Date:

04/21/08

SUBJ: Sensitive Compartmented Information (SCI) Program Management

1. **Purpose.** Revision of Chapter 3, Foreign Travel Requirements to further enhance the requirements of International travel for SCI indoctrinated FAA personnel.
2. **Explanation of Change.** The revised Chapter 3 establishes the requirement for FAA SCI indoctrinated personnel to report travel outside of the United States to AEO-300 for submission to the Office of Security, Central Intelligence Agency and affords personnel the opportunity to receive a Defensive Travel Briefing or Threat Briefing depending on the Threat level of the country to be visited. The Foreign Travel Form, Appendix G, has been incorporated in the order and will be completed within 14 days prior to travel and forwarded to AEO-300.
3. **Who this change affects.** All FAA SCI indoctrinated personnel.
4. **Disposition of Transmittal Paragraph.** Retain this change until Order 1600.76 is cancelled or superseded.

PAGE CHANGE CONTROL CHART

Remove Pages	Dated	Insert Pages	Dated
2-3	05/04/07	2-3	04/21/08
12	05/04/07	12-13	04/21/08
Remove pages 13-29		Renumbered pages 13-29	04/21/08
		31-32, Appendix G	04/21/08

5. **Administrative Information.** Appendix G form is located in the National Security Coordination Division, AEO-300.

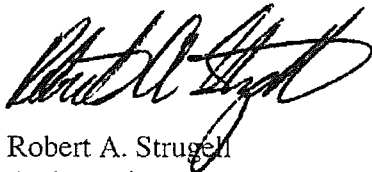

Robert A. Strugell
Acting Administrator

TABLE OF CONTENT

Chapter 1. General Information

1. What is the purpose of this order?	4
2. Who this order affects?	4
3. What document does this order cancel?	4
4. What is Sensitive Compartmented Information (SCI)?	4
5. What is the clearance requirement for access to SCI?	4
6. What responsibilities do FAA offices and individuals have for this order?	4
7. What Federal Laws, regulations, and guidance primarily apply to this order?	7

Chapter 2. Clearance Requirement and Access

1. When will a person obtain SCI access?	8
2. What are the basic requirements for SCI access?	8
3. What is need to know?	8
4. What is the process for submission of SCI access to CIA?	8
5. What are the eligibility requirements for SCI access?	8
6. What are the procedures for requesting SCI access to AEO-300?	9
7. What are the ASH procedures for verifying clearance for SCI access?	9
8. What is submitted to the Central Intelligence Agency?	10
9. What happens upon approval or disapproval of a request for SCI access?	10
10. What is an SCI Indoctrination?	10
11. What is the requirement to maintain SCI access?	11

Chapter 3. Foreign Travel Reporting Requirements

1. What are the foreign travel reporting requirements?	12
2. What are the foreign contact reporting requirements?	13

Charter 4. Physical Security

1. What is a Sensitive Compartmented Information Facility (SCIF)?	14
2. What are the requirements for a SCIF?	14
3. Who is the approval authority for a SCIF for FAA?	14
4. Who is the FAA point of contact for SCIF accreditation?	14

Chapter 5. Sensitive Compartmented Information Protective Measures

1. Why are there protective measures?	16
2. How do I protective sensitive compartmented information?	16
3. How do I package SCI material?	16
4. How do I mark SCI information?	17
5. Can SCI information be transmitted electronically?	
6. How is SCI destroyed?	17
7. Are there other requirements for protecting SCI?	17

Chapter 6. Information Systems

- | | | |
|----|--|----|
| 1. | What are the protective measures for SCI on an information system? | 19 |
| 2. | Who is the principal accrediting authority? | 19 |
| 3. | Who is the focal point for IS within FAA SCIF? | 19 |
| 4. | What is an information Security System Plan? | 19 |

Chapter 7. Security Awareness

- | | | |
|----|--|----|
| 1. | What is security awareness? | 20 |
| 2. | What are the requirements for SCI security awareness training? | 20 |
| 3. | What does the training consist of? | 20 |

Chapter 8. Administrative Information

- | | | |
|----|--|----|
| 1. | Distribution of this order | 21 |
| 2. | Who has Authority to Change or Supplement this order? | 21 |
| 3. | Who do I contact if I have questions about this order? | 21 |
| 4. | Where do I find more information about this order? | 21 |

Appendices

- | | |
|---|-------|
| Appendix A. Definition of Terms | 22-24 |
| Appendix B. Federal Laws, regulations, and guidance | 25 |
| Appendix C. Letter of Compelling Need (LCN) | 26 |
| Appendix D. Scope of Personnel Security Investigations | 27 |
| Appendix E. Memorandum Sample - Request for Sensitive Compartmented Information (SCI) Access | 28 |
| Appendix F. Sensitive Compartmented Information Nondisclosure Agreement, Form 4414 | 29 |
| Appendix G. Foreign Travel Reporting Form | 31-32 |

Chapter 3. Foreign Travel Reporting Requirements

1. What are the *foreign travel* reporting requirements?

a. FAA employees with access to SCI planning official or non-official foreign travel are required to notify the National Security Coordination Division (AEO-300), at e-mail address 'AWA-ASH-AEO-300-Travel Security, in writing, of foreign travel at least 14 days before departure. Employees will notify AEO-300 using the Foreign Travel Form (Appendix G). SCI indoctrinated employees must also provide the AEO-300 a detailed itinerary 7 to 10 days in advance of travel.

b. Non-official travel to countries that would expose the cleared employee to unnecessary risk (e.g. terrorist targeting of U.S. citizens or government representatives overseas) should be avoided.

c. FAA SCI-indoctrinated travelers will receive a defensive travel security briefing prior to foreign travel. A defensive travel security briefing alerts personnel to the potential threat from terrorists and intelligence services and provides guidance and courses of action to mitigate risk in adverse security environments. FAA SCI-indoctrinated travelers will receive a country specific threat assessment briefing prior to foreign travel to countries where there is a critical or high threat environment for U.S. citizens.

d. FAA SCI-indoctrinated persons are encouraged to visit the U.S. Department of State (DS) (www.state.gov) website to review Travel Warnings and Public Announcements for countries they anticipate visiting. These messages are issued when the State Department recommends that Americans avoid or defer travel to a country, or to alert Americans to be vigilant when traveling to specific areas of that country. In addition to this list, the State Department issues Consular Information Sheets for every country of the world with information on such matters as the health conditions, crime, unusual currency or entry requirements, any areas of instability, and the location of the nearest U.S. embassy or consulate in the subject country. Finally, the FAA SCI-indoctrinated traveler needs to review and abide by the guidance in the U.S. Embassy country clearance approval message.

e. Government-issued storage media, personal electronic devices, and notebook computers that contain classified and/or sensitive information in digital form must be protected at all times during non-domestic travel. They must be not left unattended in hotel rooms or at meetings held outside of US Department of State or US military facilities, nor should they be out of sight and inaccessible to you when traveling on commercial aircraft, trains, or buses. Upon return to a domestic FAA facility, you must submit all such electronic media and devices to your Information Systems Security Manager (ISSM) or designee to be scanned for malware before they are reconnected to any FAA information system or network.

f. If a security incident occurs, it is not recommended that the FAA traveler try to communicate the incident via telephone or internet while in-country to either FAA or the U.S. Embassy. Instead, the traveler should meet with the U.S. Embassy Regional Security Officer and report the information in person within 24 hours of the incident. Upon return from travel,

immediately (first business day) report to their immediate supervisor and SSO any unusual incidents of potential security/counterintelligence concern encountered during such travel, regardless of country(ies) visited.

g. FAA SCI-indoctrinated employees should not visit the diplomatic or trade missions of countries designated by the Department of State as sponsors of terrorism (Cuba, Iran, North Korea, Sudan and Syria), as well as travel on transport carriers owned or controlled by these countries.

2. What are the *foreign contact* reporting requirements?

a. FAA SCI-indoctrinated personnel must protect themselves against approaches and possible exploitation by foreign nationals who are or may be associated with foreign intelligence services, or organizations that support terrorism, and to whom they might unwittingly provide sensitive or classified national security information.

b. Persons with a SCI access have a continuing responsibility to report within one business day to their immediate supervisor and SSO all foreign or otherwise suspicious contacts:

(1) with representatives or citizens of foreign countries that are considered as threatening to U.S. interests.

(2) with persons from other countries whenever those persons express or pursue information regarding national security matters or sensitive agency internal or operational issues.

(3) of a close, continuing personal association, characterized by ties of kinship, affection, or obligation with foreign nationals. Casual contacts and association arising from living in a community normally need not be reported.

(4) in which illegal or unauthorized access is sought to classified, sensitive, or proprietary information or technology, either within or outside the scope of the employee's official activities. Personnel should be alert and suspicious of requests for information that exceed the scope of normal, routine business inquiries or exchanges.

c. Please note these instructions are not intended to inhibit or discourage contact with foreign nationals. They are meant to ensure that the nature of the contacts and association and all relevant information developed are properly documented. Failure to report foreign contacts will result in reevaluation of eligibility for continued SCI access by the Assistant Administrator for Security & Hazardous Materials (ASH-1) and the CIA.

Chapter 4. Physical Security

1. What is a Sensitive Compartmented Information Facility (SCIF)? A SCIF is an accredited area, room, group of rooms, buildings, or installation where SCI may be used, stored, discussed and/or processed. SCIF procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular SCI authorized for use or storage within the SCIF.

a. All SCI material will be stored, used, discussed, and/or electronically processed within an accredited SCIF.

b. FAA organizations will request the establishment of a SCIF only when there are a clear operational requirements and when existing SCIF's are not adequate to support the requirements.

c. FAA organizations will make use of existing SCIF's or consolidate SCIF's whenever possible.

2. What are the requirements for a SCIF? The requirements justifying a new SCIF will be documented and maintained with accreditation records. When it is determined that a SCIF is necessary for an SCI program, the FAA organizations will contact AEO-300 and provide justification detailing the requirement for the SCIF establishment.

3. Who is the approval authority for SCIF's for FAA? The CIA is the accreditation authority for SCIF's. Upon coordination and approval from ASH-1, AEO-300 provides a Preconstruction Request and Fixed Facility Checklist, completed by AEO-300 to the maximum extent possible, to the approval authority to review and approve to proceed with the establishment of a SCIF.

4. Who is the FAA point of contact for SCIF accreditation? The National Security Coordination Division, AEO-300, is the FAA focal point for SCIF accreditation.

a. AEO-300 SSO will ensure the SCIF is constructed in accordance with the security specification provided in the DCID 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities*. Upon completion of construction, the SSO will ensure an inspection is conducted with the CIA to ensure it meets standards.

b. The SSO will ensure a TEMPEST inspection (if applicable) is conducted in accredited SCIFs as necessary. The SSO will ensure a Technical Surveillance Countermeasures (TSCM) survey is requested when the following circumstances occur:

- (1) New construction of a SCI Facility
- (2) Damage or modification to a SCI Facility
- (3) SCI Facility is found unsecured

c. The CIA will conduct a final inspection of the SCIF, and review and approve the required SCIF documentation and procedures. SCIF accreditation documentation will be approved by CIA.

d. The SSO will obtain approval from the CIA for any significant changes regarding the integrity of any CIA-accredited SCIF, prior to any changes in the SCIF construction or operating procedures. These may include, but are not limited to, changes in perimeter, alarms, or anything that might introduce a vulnerability to the facility.

e. SCIF construction costs will be funded by the customer/user.

Chapter 5. Sensitive Compartmented Information Protective Measures

1. Why are there Protective Measures? Protective measures are used to safeguard SCI from inadvertent disclosure to personnel outside the FAA, and inadvertent dissemination and disclosure within the FAA. Protective measures start with marking and end with destruction.

2. How do I Protect Sensitive Compartmented Information?

a. Handling. SCI will only be discussed, used, handled, electronically processed, or stored within an accredited SCIF.

b. Physical Control. SCI material will not be sent to a facility or building that does not have a SCIF, or to an individual who does not have access to SCI.

c. Courier. SCI material sent between accredited SCIF's will be hand-carried by individuals who are properly briefed on courier procedures, possess a valid courier card or letter, and who are cleared for the material being transported.

3. How do I Package SCI Material?

a. Materials carried within a building should be in a sealed opaque envelope that is properly addressed.

b. SCI will be enclosed for shipment in two opaque envelopes or otherwise suitably double-wrapped using approved containers.

c. Outer containers will be secured by an approved means that reasonably protects against surreptitious access. The inner and other containers shall be annotated to show the package number and addresses of the sending and receiving SCIF. The notation "TO BE OPENED BY THE (appropriate SCI SSO)" must be placed above the pouch address of the receiving SCIF on the inner container. The inner wrapper must contain the document receipt and name of the person or activity for which the material is intended. The applicable security classification and the legend "CONTAINS SENSITIVE COMPARTMENTED INFORMATION" must appear on each side of the inner wrapper only.

d. Materials transported between buildings will be doubled-wrapped in the same manner required for National Security Information.

4. How do I Mark SCI Information? All SCI materials will be properly marked and, when required, have cover sheets attached.

a. Dissemination Control Markings. When applicable to its information content, SCI documents will be marked with the dissemination control markings in the manner prescribed by DCID 6/6, *Security Controls on the Dissemination of Intelligence Information*.

b. **Portion Marking.** SCI documents will, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are not classified and, which portions require SCI code words, caveats, program designators, or DCID 6/6 control markings.

5. Can SCI Information be Transmitted Electronically? Electronic transmission of SCI will be limited to specifically designated and accredited communications circuits secured by NSA-approved cryptographic systems and/or protected distribution systems. SCI transmitted electrically or electronically (to include facsimile, computer, secure voice, E-mail, or any other means of telecommunications), must ensure that such transmissions are made only to authorized recipients. Recipients of SCI information must provide proper protection for material received.

a. SCI can be processed only on a computer, or network of computers, that has been specifically certified and accredited for that level of classified information.

b. SCI materials may be electronically transferred between appropriately accredited machines (facsimile, computers, secure voice, secure e-mail, or any other means of telecommunications) ensuring that such transmissions are made only to authorized recipients.

c. It is essential to ensure that appropriate secure devices are used for any transfer of SCI material.

6. How is SCI Destroyed? Destruction of SCI will be accomplished in a manner that will preclude reconstruction in intelligible form. Only those DCI approved methods (e.g. burning, pulping, shredding, pulverizing, melting, or chemical decomposition, depending on the type of material to be destroyed) specifically authorized may be used.

7. Are there other requirements for protecting SCI?

a. **Public Media.** SCI will not be released to, or discussed with the media. FAA is not authorized to declassify SCI for public release without the prior written approval of the appropriate Director, Central Intelligence Executive Agent.

b. **Public Declaration.** Disclosure of SCI appearing in the media, publications, or other sources does not alter the basic security policies and procedures contained in the DCID's. Persons will not confirm nor deny any information they are questioned about regarding information in the media, publications, or other sources. Such information remains classified until such time that it is deemed declassified or releasable. Individuals are not relieved of their obligation to maintain the secrecy of such information and are bound by the Nondisclosure Agreement.

c. Pre-Publication Review. Pre-publication review is required for classification and policy review prior to release of SCI-related information. Such pre-publication review is also necessary to avoid potential damage that would result from confirmation of previously published information containing SCI.

Chapter 6. Information Systems

1. What are the Protective Measures for SCI on an Information System? The Director, Central Intelligence, requires all United States Government departments, agencies, and their contractors processing intelligence information to establish, implement, maintain, and abide by the protective measures for SCI. All telecommunications and automated information systems (AIS) used to process and store SCI within FAA, must be protected against unauthorized disclosure, modification, access, use, destruction, or delay in service.

2. Who is the Principal Accrediting Authority for Information Systems? The principal accrediting authority for information systems that processes intelligence information for FAA is the CIA. All AIS that process, store, or handle SCI will be certified and accredited by CIA prior to operation to ensure compliance delineated in the DCID 6/3, *Protecting Sensitive Compartmented Information within Information Systems*.

3. Who is the Focal Point for Information Systems within a SCIF? The National Security Division, AEO-300, is the FAA point of contact for information systems for processing SCI within FAA.

a. SCI systems will not be placed in operation until authorized, in writing, by the CIA.

b. When the need to obtain AIS for processing SCI information becomes apparent, AEO-300 will contact the CIA for certification and accreditation assessment.

c. AEO-300 in concert with the Systems Administrator will provide support in defining the organizational needs and the requirements necessary to meet those needs. The Systems Administrator will provide support to the CIA in developing security-related documentation for the certification and accreditation process and the preparation of an information system.

4. What is an Information Security System Plan (ISSP)? The ISSP identifies information system components, operational environment, sensitivity and risks, and detailed, cost-effective measures to protect a system and the information it contains. Commensurate with the risk and magnitude of harm from unauthorized disclosure, the ISSP spells out measures to protect SCI within the system.

Chapter 7. Security Awareness Programs

1. What is Security Awareness? Security awareness is the continued process of providing information, training, and education for the protection of employees, facilities, and classified information. The DCID 6/1, *Security Policy for Sensitive Compartmented Information and Security Policy Manual*, establishes the security awareness requirements for the U.S. Intelligence Community.

2. What is the Requirement for SCI Security Awareness Training? The SSO will establish a continuing security awareness program that will provide frequent exposure of security awareness material for SCI indoctrinated personnel. The program may include live briefings, audio-visual presentations, printed material, or a combination thereof. The security awareness program will be designed to meet the particular needs of the agency.

3. What Does The Training Consist Of? The basic elements for this program include, but are not limited to the following:

- a. Foreign intelligence and technical threat.
- b. A reminder to report outside activities, foreign travel, and foreign contacts, as required.
- c. Individual classification management responsibilities.
- d. A reminder that FAA SCI-indoctrinated individuals are required to inform the SSO about any personal problems or situation which may have a bearing on their eligibility for continued access to SCI.
- e. A reminder that FAA SCI-indoctrinated individuals are required to inform the SSO about any changes in their personal status which may have a possible bearing on their eligibility for continued access to SCI.
- f. A reminder to FAA SCI-indoctrinated individuals to report any information to AEO-300 and AIN-400 which may adversely affect both SCI and security/suitability of an individual.
- g. A reminder of the prepublication review.

Chapter 8. Administrative Information

1. Distribution of This Order: This order is distributed to branch level and above at the Washington Headquarters; branch level and above at the Mike Monroney Aeronautical Center, FAA Technical Center, and all field facilities; and all FAA contract towers. This order is also electronically available at <http://dmis.faa.gov>.

2. Who has Authority to Change or Supplement This Order?

a. Changes. The Assistant Administrator for Security and Hazardous Materials issues changes which do not modify the FAA policy, delegation of authority, assignment of responsibility, or have a significant impact on resource requirements.

b. Supplements. The Assistant Administrator for Security and Hazardous Materials issues changes which do not modify FAA policy, delegation of authority, assignment of responsibility, or have a significant impact on resource requirements.

3. Who do I Contact if I have a Question About This Order? The National Security Coordination Division, AEO-300.

4. Where do I Find More Information About This Order?

a. Federal laws, regulations and guidance. See Appendix B.

b. FAA orders and policies. See Appendix B.

Appendix A - Definition of Terms

- 1. Access Approval.** When **need-to-know** has been established, investigative results have been satisfactorily adjudicated, and an authorized NdA has been signed, SCI access shall be granted and officially recorded. When a previous need-to-know no longer exists due to reorganization, reassignment, change in duties or any other reason, the SCI access approval(s) affected by this change in **need-to-know** shall be canceled, and the individual involved debriefed.
- 2. Accreditation:** The formal certification by the CSA that a facility meets prescribed DCID 6/9 physical and technical security standards.
- 3. Adjudicate or Adjudication:** The process of determining one's SCI eligibility or ineligibility.
- 4. Cognizant Security Authority.** Intelligence organizations or agencies as defined in E.O. 12333, that have the authority and are responsible for all aspects of security program management with respect to the protection of intelligence sources and methods, and implementation of the DCID's for activities under their purview.
- 5. Compelling Need.** A signed determination by a Senior Official of the Intelligence Community or designee, that services of an individual are deemed essential to operation or mission accomplishment.
- 6. Defensive Security Briefing.** Formal advisories intended to minimize the risk to SCI that include information on: (1) course of action helpful in mitigating adverse security and personal situations, and (2) active and passive measures that personnel should take to avoid becoming targets or inadvertent victims as a consequence of foreign travel. To the extent possible, these advisories will be based upon current and continuously updated counterintelligence threat information.
- 7. Director, Central Intelligence Directive.** A directive issued by the Director, Central Intelligence which outlines policies and procedures to be followed by intelligence agencies and organizations which are under his direction or overview. The DCI has statutory responsibility for the protection of intelligence sources and methods.
- 8. Indoctrination.** The initial instructions concerning the unique nature of SCI, its unusual sensitivity, and the special security regulations and practices for its handling which is given to each individual who has been approved for access prior to his/her exposure.
- 9. Intelligence Community.** United States Government agencies and organizations and activities identified in Section 3 of the National Security Act of 1947 and Section 3.4(F) (1 through 6) of Executive Order 12333.

10. National Agency Check. An integral part of all background investigations, consisting of searches of the OPM Security/Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation (FBI) Identification Division's name and fingerprint files, and other files or indices when necessary.

11. 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 a lawful and authorized function. Such person shall possess an appropriate security clearance and access approvals in accordance with DCID 6/4.

12. Nondisclosure Agreement. A written, legally binding agreement (Form 4414) signed by a candidate for SCI access. The candidate promises not to disclosure SCI to unauthorized individuals.

13. Official Travel. Travel performed at the direction of the U.S. Government

14. Periodic Reinvestigation. An investigation conducted at a specified interval for the purpose of updating a previously completed background investigation, special background investigation, single scope background investigation, or Periodic Reinvestigation.

15. Security Clearance. A formal authorization for an employee with a specific "need-to-know" to have access to information that is classified as Confidential, Secret, or Top Secret in the interest of national security or the defense of the United States.

16. Senior Intelligence Officer. The highest ranking military or civilian individual charged with direct foreign intelligence missions, functions, or responsibilities within a department, agency, component, command, or element of an Intelligence Community organization.

17. Senior Officials of the Intelligence Community. The head of an agency, office, bureau, or intelligence element listed in Section 3.4f (1 through 8) of Executive Order 12333.

18. Sensitive Compartmented Information. Classified information concerning or derived from intelligence sources, methods, or analytical processes requiring handling within formal access control systems established by the DCI. SCI is also referred to as "codeword" information. The sensitivity of this information requires that it be protected in a much more controlled environment than other classified information. Therefore, the DCI has established special policies and procedures for the protection of SCI. These policies and procedures promulgated through DCID's.

19. Sensitive Compartmented Information Facility. An accredited area, room, group of rooms, buildings, or installation where SCI may be used, stored, discussed and/or processed. SCIF procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular SCI authorized for use of storage within the SCIF.

20. Single Scope Background Investigation. An investigation completed according to agency regulations, meeting the investigative scope requirements for SCI access. A personnel security investigation consisting of the following investigative requirements: NAC, spouse NAC, subject interview; birth/citizenship checks; education, employment, local agency, public record and credit record checks; neighborhood, employment, listed and developed character reference interviews, accomplished with a ten-year scope. Final SCI adjudication will be held in abeyance pending completion of the investigation.

21. Special Security Officer. The SSO is responsible for the security management, operation, implementation, use and dissemination of all communications intelligence and other types of SCI material within his/her respective organization.

22. Suspension of Access: The temporary withdrawal of a person's eligibility for access to classified information when information becomes known that casts doubt as to whether continued access is consistent with the best interests of national security.

23. Unofficial Travel. Travel that is undertaken by an individual without official, fiscal, or other obligations on the part of the United States Government.

Appendix B - Authorities

This order is governed by the following Executive Orders, DCID's, and FAA authorities:

- a. The National Security Act of 1947, as amended
- b. Executive Order 12333, United States Intelligence Activities
- c. Executive Order 12968, Access to Classified Information
- d. Executive Order 12958, as amended "Classified National Security Information"
- e. Executive Order 12829, National Industrial Security Program
- f. DCID 6/1, Security Policy for Sensitive Compartmented Information and Security Policy Manual
- g. DCID 6/3, Protecting Sensitive Compartment Information within Information Systems
- h. DCID 6/4, Personnel Security Standards and Procedures Governing Eligibility For Access to Sensitive Compartmented Information
- i. DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities
- j. FAA Order 1600.1 Personnel Security Program
- k. FAA Order 1660.12, Technical Surveillance Countermeasures (TSCM) Program
- k. FAA Order 1600.61, International Travel Security Briefings & Contact Reporting Requirements for FAA Employees and Contractors

Appendix C - Exemplar - Letter of Compelling Need

It is our understanding that the (spouse, siblings, parents etc.) of Subject's Name are foreign nationals. Please be advised that *(requesting agency's name)* has a need for *Mr/Ms* _____'s services.

Provide a Brief explanation of Subject's value to the mission (i.e. why he/she is the only individual available with a given skill or expertise)

Because of *(requesting agency's name)* critical need for (Subject's role/professional credentials/expertise, etc.), it is requested that the DCID 6/4 requirement that Mr/Ms' (spouse, sibling, parents, etc) be U.S. citizens be waived.

Appendix D - Scope of Personnel Security Investigations

1. Single Scope Background Investigation: The period of investigation is the last 10 years of the subject's life or back to the 18th birthday whichever is shorter. In any case, the investigation will cover at least two full years of the subject's life, but no investigation will be conducted before the 16th birthday. (This means that a subject must be at least 18 years old to have an SSBI). FAA will conduct any investigative leads necessary to resolve issues raised by the SSBI.

2. Elements of the SSBI:

- a. Last 10 years
- b. ANAC
- c. Spouse NAC
- d. Subject Interview
- e. Employment Records
- f. Employment Interviews
- g. Military Service and Discharge Verified
- h. Developed Character References
- i. Listed Character References
- j. Neighborhood Interviews
- k. Local Agency Checks
- l. Credit Checks
- m. Ex-Spouse Interviews

3. Single Scope Periodic Reinvestigation (SSBI-PR): The purpose of the PR is to update the SSBI. Its period of investigation is the last five years of subject's life. FAA will conduct any investigative leads necessary to resolve issues that are raised in the course of the PR.

4. Elements of The PR:

- a. Last 5 years
- b. NAC
- c. Spouse NAC
- d. Subject Interview
- e. Employment Records
- f. Employment Interviews
- g. Developed Character References
- h. Neighborhood Interviews
- i. Local Agency Checks
- j. Credit Checks

Appendix E – SCI Nomination Sample Memorandum

SUBJECT: Request for SCI Clearance for Employee Assigned to _____

FROM: Manager, Justifying Office

TO: Manager, National Security Coordination Division

Summary:

Request that Name, SSN, be processed for access to Sensitive Compartmented Information (SCI) or list additional access(es). Mr/Ms (Name) is assigned to the Office of _____, Federal Aviation Administration and has the duty title of (position and/or function). Successful performance of assigned duties/functions requires that (Name) hold a Top Secret Clearance with SCI access in order to performed required duties. Mr/Mrs (Name) currently holds a Top Secret clearance (date of clearance and who granted it).

Justification:

Personnel assigned to the FAA Office of Name of Office are responsible for performing liaison with a host of U.S. Government (list these agencies) to coordinate and resolves related issues to the Federal Aviation Administration security.

Identify all pertinent information required to gain approval for SCI or additional accesses:

- (Name) is the office's primary liaison with
- (Name) often attends meetings
- (Name) requires access to SCI in the performance of his/her duties.
- (Name) office is located in a Sensitive Compartment Information Facility (SCIF).

Signature Block of Key Director

SFN _____

SENSITIVE COMPARTMENTED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement Between _____

(Name—Printed or Typed)

and the United States

1 Intending to be legally bound I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information or material protected within Special Access Programs hereinafter referred to in this Agreement as Sensitive Compartmented Information (SCI) I have been advised that SCI involves or derives from intelligence sources or methods and is classified or is in the process of a classification determination under the standards of Executive Order 12356 or other Executive order or statute I understand and accept that by being granted access to SCI special confidence and trust shall be placed in me by the United States Government

2 I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information or material have been approved for access to it and I understand these procedures I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SCI I further understand that all my obligations under this Agreement continue to exist whether or not I am required to sign such subsequent agreements

3 I have been advised that the unauthorized disclosure unauthorized retention or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that last authorized my access to SCI I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized my access to SCI whether or not I am still employed by or associated with that Department or Agency or a contractor thereof in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be SCI or related to or derived from SCI is considered by such Department or Agency to be SCI I further understand that I am also obligated by law and regulation not to disclose any classified information or material in an unauthorized fashion

4 In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access to SCI I hereby agree to submit for security review by the Department or Agency that last authorized my access to such information or material any writing or other preparation in any form, including a work of fiction that contains or purports to contain any SCI or description of activities that produce or relate to SCI or that I have reason to believe are derived from SCI that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure I understand and agree that my obligation to submit such preparations for review applies during the course of my access to SCI and thereafter and I agree to make any required submissions prior to discussing the preparation with or showing it to anyone who is not authorized to have access to SCI I further agree that I will not disclose the contents of such preparation to any person not authorized to have access to SCI until I have received written authorization from the Department or Agency that last authorized my access to SCI that such disclosure is permitted

5 I understand that the purpose of the review described in paragraph 4 is to give the United States a reasonable opportunity to determine whether the preparation submitted pursuant to paragraph 4 sets forth any SCI I further understand that the Department or Agency to which I have made a submission will act upon it coordinating within the Intelligence Community when appropriate and make a response to me within a reasonable time not to exceed 30 working days from date of receipt

6 I have been advised that any breach of this Agreement may result in the termination of my access to SCI and removal from a position of special confidence and trust requiring such access as well as the termination of my employment or other relationships with any Department or Agency that provides me with access to SCI In addition I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws including the provisions of Sections 793 794 798 and 952 Title 18 United States Code and of Section 783(b) Title 50 United States Code Nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation

7 I understand that the United States Government may seek any remedy available to it to enforce this Agreement including but not limited to application for a court order prohibiting disclosure of information in breach of this Agreement I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action Court costs and reasonable attorneys fees incurred by the United States Government may be assessed against me if I lose such action

8 I understand that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law Subject to such determination I do not now nor will I ever possess any right interest title or claim whatsoever to such information I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials If I do not return such materials upon request I understand this may be a violation of Section 793 Title 18 United States Code

9 Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me with access to SCI I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to SCI and at all times thereafter

10 Each provision of this Agreement is severable If a court should find any provision of this Agreement to be unenforceable all other provisions of this Agreement shall remain in full force and effect This Agreement concerns SCI and does not set forth such other conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency

11 I have read this Agreement carefully and my questions if any have been answered to my satisfaction I acknowledge that the briefing officer has made available Sections 793 794 798 and 952 of Title 18 United States Code and Section 783(b) of Title 50 United States Code and Executive Order 12356 as amended so that I may read them at this time if I so choose

CRM 9 4414 People F0 in 4 no
wh h s t e u a n d i a
not t sed)

Appendix F. Sensitive Compartmented Information Non Disclosure Agreement

12. I hereby assign to the United States Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.

13. These restrictions are consistent with and do not supersede conflict with or otherwise alter the employee obligations rights or liabilities created by Executive Order 12333; section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosures to Congress by members of the Military); section 2302(b)(8) of title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including section 641, 793, 794, 798, and 952 of title 18, United States Code, and section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

14. This Agreement shall be interpreted under and in conformance with the law of the United States.

15. I make this Agreement without any mental reservation or purpose of evasion.

Signature

Date

The execution of this Agreement was witnessed by the undersigned who accepted it on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information.

WITNESS and ACCEPTANCE:

Signature

Date

SECURITY BRIEFING / DEBRIEFING ACKNOWLEDGMENT		
<div style="display: flex; justify-content: space-between; margin-bottom: 10px;"> <div>_____</div> <div>_____</div> <div>_____</div> </div> <div style="display: flex; justify-content: space-between; margin-bottom: 10px;"> <div>_____</div> <div>_____</div> <div>_____</div> </div> <p style="text-align: center;">(Special Access Programs by Initials Only)</p> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div>_____</div> <div>_____</div> <div>_____</div> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div>SSN (See Notice Below)</div> <div>Printed or Typed Name</div> <div>Organization</div> </div>		
<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>BRIEF DATE _____</p> <p>I hereby acknowledge that I was briefed on the above SCI Special Access Programs(s):</p> <p>_____ Signature of Individual Briefed</p> </div>	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>DEBRIEF DATE _____</p> <p>Having been reminded of my continuing obligation to comply with the terms of this Agreement, I hereby acknowledge that I was debriefed on the above SCI Special Access Programs(s):</p> <p>_____ Signature of Individual Debriefed</p> </div>	
<p>I certify that the briefing presented by me on the above date was in accordance with relevant SCI procedures.</p> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div>_____</div> <div>_____</div> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div>Signature of Briefing/Debriefing Officer</div> <div>SSN (See Notice Below)</div> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div>_____</div> <div>_____</div> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div>Printed or Typed Name</div> <div>Organization (Name and Address)</div> </div>		

NOTICE: The Privacy Act, 5 U.S.C. 522a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, 2) determine that your access to the information indicated has terminated, or certify that you have witnessed a briefing or debriefing. Although disclosure of your SSN is not mandatory, your failure to do so may impede such certification or determinations.

Appendix G - Foreign Travel Reporting Form
(OFFICIAL/PERSONAL OVERSEAS TRAVEL)

Employee Information:

Date: _____

Employee Name: _____

Supervisor Name: _____

Agency/LOB: _____

Office Address: _____ Phone: _____

Travel Information:

Destination: _____

Dates of Travel: _____

Beginning Date: _____

Return Date: _____

Purpose of Travel: _____

Dependents or Traveling Companion: YES _____ NO _____

Names/Relationships: _____

Emergency Notification Name: _____

Work Phone: _____

Member SIGNATURE _____

Appendix G - Foreign Travel Reporting Form
ITINERARY - Continuation**LEG 1 Itinerary****Attachment of Electronic Ticket (E-ticket) is acceptable.**

Airline/Cruise: _____ Flight Number: _____
Departure Date: _____ Departure City: _____
Destination City: _____ Destination Country: _____
Foreign National Contacts: _____
Alternate modes of transportation, charter flight information, comments, etc: _____

LEG 2 Itinerary

Airline/Cruise: _____ Flight Number: _____
Departure Date: _____ Departure City: _____
Destination City: _____ Destination Country: _____
Foreign National Contacts: _____
Alternate modes of transportation, charter flight information, comments, etc: _____

LEG 3 Itinerary

Airline/Cruise: _____ Flight Number: _____
Departure Date: _____ Departure City: _____
Destination City: _____ Destination Country: _____
Foreign National Contacts: _____
Alternate modes of transportation, charter flight information, comments, etc: _____

LEG 4 Itinerary

Airline/Cruise: _____ Flight Number: _____
Departure Date: _____ Departure City: _____
Destination City: _____ Destination Country: _____
Foreign National Contacts: _____
Alternate modes of transportation, charter flight information, comments, etc: _____

Supervisor's Signature/Date/Comments: _____
Security