This manual is the property of the Federal Bureau of Investigation and may not be released outside the FBI without approval from the FBI’s Security Division. The FBI retains ownership of this manual even when released, and its contents are not to be distributed by anyone other than the FBI. This manual contains information exempt from mandatory disclosure under the Freedom of Information Act, Exemption 2.
GENERAL INFORMATION: Questions or comments pertaining to this manual can be directed to:

HQ FBI /Security Division, Division 11
Mission Support Section, Analysis and Policy Unit

(NOTE: This document supersedes all existing security policy contained in the MAOP and MIOG.)
Table of Contents

Scope ................................................................................................................................. 1
Key Terms and Acronyms ................................................................................................. 2
Summary of Legal Authorities .......................................................................................... 5
Roles and Functional Responsibilities ............................................................................... 6

1. Individuals ....................................................................................................................... 6
2. Assistant Director, Security Division ............................................................................... 6
3. Assistant Directors and Special Agents in Charge (Division Heads) ............................. 7
4. Chief Information Officer (CIO) ..................................................................................... 8
5. Chief Security Officers (CSO) ....................................................................................... 8
6. Information System Security Manager (ISSM) ........................................................... 9
7. Information System Security Officer (ISSO) ............................................................... 9
8. System Administrator ..................................................................................................... 9
9. All Supervisors ................................................................................................................ 9

Policies .................................................................................................................................. 10

1. Security Management .................................................................................................... 10
   1.1. Purpose ..................................................................................................................... 10
   1.2. General .................................................................................................................... 10
   1.3. Risk Management .................................................................................................... 10
   1.4. Dissemination and Disclosure under Emergency Conditions ........................... 11
   1.5. Public Declarations ................................................................................................. 11
   1.6. Foreign Disclosure .................................................................................................. 12
   1.7. Standard Operating Procedures (SOP) ................................................................. 12
   1.8. Inspections ............................................................................................................. 12
   1.9. Security Awareness Program .................................................................................. 13
   1.11. Security Coordination Requirement ..................................................................... 16
   1.12. Off-Site Conferences ............................................................................................ 16
   1.13. Policy Waivers and Exceptions ............................................................................ 17
   1.14. Field Personnel Files ............................................................................................ 18
   1.15. Lock Combination Procedures ............................................................................ 19

2. Personnel Security .......................................................................................................... 22
   2.1. Purpose ................................................................................................................... 22
   2.2. Policy ...................................................................................................................... 22
   2.3. Effective Date: 04/24/2009.Requirements for Clearance and Access .................. 22
   2.4. Personnel Security Interviews .............................................................................. 24
   2.5. Non Disclosure Agreement .................................................................................... 24
   2.6. Indoctrination for Access ........................................................................................ 24
   2.7. Reciprocity ............................................................................................................. 24
   2.8. One Time Access ................................................................................................... 25
   2.9. Interim Clearance ................................................................................................... 25
   2.10. Inadvertent Disclosure .......................................................................................... 25
   2.11. Denial or Revocation of Clearance/Access ........................................................... 25
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.12</td>
<td>Clearance Passage</td>
</tr>
<tr>
<td>2.13</td>
<td>Sensitive Compartmented Information (SCI) Access</td>
</tr>
<tr>
<td>2.14</td>
<td>Debrief from SCI Accesses and Clearances</td>
</tr>
<tr>
<td>2.15</td>
<td>Outside Indoctrination Assistance</td>
</tr>
<tr>
<td>2.16</td>
<td>Reinvestigations</td>
</tr>
<tr>
<td>2.17</td>
<td>Exit Interviews</td>
</tr>
<tr>
<td>2.18</td>
<td>Continuing Clearance for Retiring FBI Officials/Personnel</td>
</tr>
<tr>
<td>2.19</td>
<td>Outside Activities</td>
</tr>
<tr>
<td>2.20</td>
<td>Cohabitant/Roommate</td>
</tr>
<tr>
<td>2.21</td>
<td>Change in Marital Status</td>
</tr>
<tr>
<td>2.22</td>
<td>Official Foreign Travel</td>
</tr>
<tr>
<td>2.23</td>
<td>Unofficial Foreign Travel</td>
</tr>
<tr>
<td>2.24</td>
<td>Foreign Contacts</td>
</tr>
<tr>
<td>2.25</td>
<td>Financial Disclosure</td>
</tr>
<tr>
<td>2.26</td>
<td>Polygraph Program</td>
</tr>
<tr>
<td>3.</td>
<td>Visitor Control</td>
</tr>
<tr>
<td>4.</td>
<td>Foreign National Access to FBI Facilities</td>
</tr>
<tr>
<td>4.1</td>
<td>Purpose</td>
</tr>
<tr>
<td>4.2</td>
<td>Policy</td>
</tr>
<tr>
<td>4.3</td>
<td>Definitions</td>
</tr>
<tr>
<td>4.4</td>
<td>Responsibilities</td>
</tr>
<tr>
<td>4.5</td>
<td>Disclosure or Release of Intelligence Information</td>
</tr>
<tr>
<td>4.6</td>
<td>Escort Requirement</td>
</tr>
<tr>
<td>4.7</td>
<td>Unexpected Foreign National Visitors</td>
</tr>
<tr>
<td>4.8</td>
<td>VIP Foreign National Visitors</td>
</tr>
<tr>
<td>4.9</td>
<td>Hosted Visits</td>
</tr>
<tr>
<td>4.10</td>
<td>Foreign National Access to SCIFs</td>
</tr>
<tr>
<td>4.11</td>
<td>Foreign National Access to Information Systems and Telephones</td>
</tr>
<tr>
<td>4.12</td>
<td>Foreign Nationals with a Security Detail</td>
</tr>
<tr>
<td>4.13</td>
<td>Vendors</td>
</tr>
<tr>
<td>4.14</td>
<td>Procedures for Foreign Visitor Access to Headquarters</td>
</tr>
<tr>
<td>4.15</td>
<td>Foreign Integrated Person (FIP)</td>
</tr>
<tr>
<td>5.</td>
<td>National Security Information</td>
</tr>
<tr>
<td>5.1</td>
<td>Purpose</td>
</tr>
<tr>
<td>5.2</td>
<td>Policy</td>
</tr>
<tr>
<td>5.3</td>
<td>Definitions</td>
</tr>
<tr>
<td>5.4</td>
<td>Classification and Declassification Authorities</td>
</tr>
<tr>
<td>5.5</td>
<td>Compilation</td>
</tr>
<tr>
<td>5.6</td>
<td>Marking Classified Information</td>
</tr>
<tr>
<td>5.7</td>
<td>Classification Prohibitions and Limitations</td>
</tr>
<tr>
<td>5.8</td>
<td>Classification Markings</td>
</tr>
<tr>
<td>5.9</td>
<td>Marking Specialized Items</td>
</tr>
<tr>
<td>5.10</td>
<td>Cover Sheets</td>
</tr>
<tr>
<td>5.11</td>
<td>Classification Challenges</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>9.5. Occupant Emergency Plans (OEP)</td>
<td>85</td>
</tr>
<tr>
<td>9.6. Emergency Destruction Identification</td>
<td>86</td>
</tr>
<tr>
<td>9.7. Security Equipment Room or Closet</td>
<td>86</td>
</tr>
<tr>
<td>10.1. Purpose</td>
<td>86</td>
</tr>
<tr>
<td>10.2. Policy</td>
<td>86</td>
</tr>
<tr>
<td>10.3. Closed Storage Area Requirements</td>
<td>87</td>
</tr>
<tr>
<td>10.4. Secure Area Approval Process</td>
<td>89</td>
</tr>
<tr>
<td>10.5. Access Control</td>
<td>89</td>
</tr>
<tr>
<td>10.6. Security Procedures</td>
<td>89</td>
</tr>
<tr>
<td>10.7. Occupant Emergency Plans (OEP)</td>
<td>90</td>
</tr>
<tr>
<td>10.8. Security Equipment Room or Closet</td>
<td>91</td>
</tr>
<tr>
<td>10.9. Open Storage Secure Areas</td>
<td>91</td>
</tr>
<tr>
<td>11. Firearms in FBI-Controlled Spaces</td>
<td>91</td>
</tr>
<tr>
<td>11.1. FBI Employees</td>
<td>91</td>
</tr>
<tr>
<td>11.2. Non-FBI Employees</td>
<td>92</td>
</tr>
<tr>
<td>12. Entry/Exit Inspection Program</td>
<td>92</td>
</tr>
<tr>
<td>12.1. Purpose</td>
<td>92</td>
</tr>
<tr>
<td>12.2. Policy</td>
<td>92</td>
</tr>
<tr>
<td>12.3. Extent of Inspections</td>
<td>92</td>
</tr>
<tr>
<td>12.4. Seized Items</td>
<td>93</td>
</tr>
<tr>
<td>12.5. Consequences of Refusals to Participate in Program</td>
<td>93</td>
</tr>
<tr>
<td>12.6. Persons Carrying Out Policy and Training</td>
<td>93</td>
</tr>
<tr>
<td>12.7. Efforts To Be Taken To Avoid Inconvenience</td>
<td>94</td>
</tr>
<tr>
<td>12.8. Notice of Subject to Searches</td>
<td>94</td>
</tr>
<tr>
<td>12.9. Magnetometer (Metal Detector) Screening</td>
<td>94</td>
</tr>
<tr>
<td>12.10. X-Ray Screening</td>
<td>94</td>
</tr>
<tr>
<td>14. Computerized Telephone Switch for Newly Constructed FBI Facilities</td>
<td>94</td>
</tr>
<tr>
<td>15. Security Review Requirements for Real Property</td>
<td>95</td>
</tr>
<tr>
<td>15.1. Purpose</td>
<td>95</td>
</tr>
<tr>
<td>15.2. Policy</td>
<td>95</td>
</tr>
<tr>
<td>15.3. Applicability</td>
<td>95</td>
</tr>
<tr>
<td>15.4. Definitions</td>
<td>95</td>
</tr>
<tr>
<td>15.5. Responsibilities</td>
<td>95</td>
</tr>
<tr>
<td>15.6. Procedures</td>
<td>96</td>
</tr>
<tr>
<td>15.7. GSA Involvement</td>
<td>97</td>
</tr>
<tr>
<td>15.8. FBI as Leasing Agent</td>
<td>97</td>
</tr>
<tr>
<td>16. Acquisition Security</td>
<td>97</td>
</tr>
<tr>
<td>16.1. Purpose</td>
<td>97</td>
</tr>
<tr>
<td>16.2. Policy</td>
<td>97</td>
</tr>
<tr>
<td>16.3. Definitions</td>
<td>98</td>
</tr>
<tr>
<td>16.4. Responsibilities</td>
<td>99</td>
</tr>
<tr>
<td>16.5. Contracts Involving Classified National Security Information (NSI)</td>
<td>100</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>24.11</td>
<td>Information System Security Manager (ISSM)</td>
</tr>
<tr>
<td>24.12</td>
<td>Information System Security Officers (ISSOs)</td>
</tr>
<tr>
<td>24.13</td>
<td>Chief Security Officer (CSO)</td>
</tr>
<tr>
<td>24.14</td>
<td>System Administrators</td>
</tr>
<tr>
<td>24.15</td>
<td>Enterprise Security Operations Center (ESOC)</td>
</tr>
<tr>
<td>24.16</td>
<td>Systems Security and Access Unit (SSAU)</td>
</tr>
<tr>
<td>24.17</td>
<td>User</td>
</tr>
<tr>
<td>24.18</td>
<td>Information System Requirements</td>
</tr>
<tr>
<td>25.</td>
<td>Information Assurance Certification and Accreditation</td>
</tr>
<tr>
<td>26.</td>
<td>Information Assurance Media Protection</td>
</tr>
<tr>
<td>27.</td>
<td>Information Assurance System and Information Integrity</td>
</tr>
<tr>
<td>28.</td>
<td>Information Assurance System and Information Integrity</td>
</tr>
<tr>
<td>28.1.</td>
<td>Purpose</td>
</tr>
<tr>
<td>28.2.</td>
<td>Policy</td>
</tr>
<tr>
<td>28.3.</td>
<td>Applicability</td>
</tr>
<tr>
<td>28.4.</td>
<td>Scope</td>
</tr>
<tr>
<td>28.5.</td>
<td>Responsibilities</td>
</tr>
</tbody>
</table>

**LIST OF APPENDICES**

- Appendix A: Definitions | A-1
- Appendix B: Keyword Acronyms | B-1
- Appendix C: Legal Authorities | C-1
- Appendix D: Hyperlinks | D-1

**LIST OF FIGURES**

- Figure 7-1. FBI Access Badges | 91

**LIST OF ATTACHMENTS**

- Attachment 4-1 Certification of Conditions and Responsibilities for Foreign Integrated Personnel
- Attachment 24-1: FBI Password Guidance | 125
Scope

Purpose. To establish a consolidated manual containing security policy for the protection of FBI people, information, operations, equipment, and facilities. This manual is broad in scope providing security policies and procedures for the protection, use, and dissemination of classified information and material, including sensitive compartmented information (SCI); personnel security; physical and technical security requirements; transmission requirements; industrial and acquisition security; force protection; security compliance; information assurance and systems security; and communication security.

The Security Division’s intent is that this manual will serve to strengthen the FBI’s stance toward security, and in the process, benefit United States national security. It is expected that this manual will allow greater ease in describing the procedures which define the FBI’s security programs, and in retrieving and understanding those specific procedures which apply to given situations. It is also intended that the processes found herein will make future betrayals through espionage less likely to occur, and be more quickly subject to discovery.

Background. This manual owes its origin to recommendations in “A Review of FBI Security Programs,” (Webster Commission Report), dated March 2002, and a Reengineering Effort of Director Robert S. Mueller III. The Security Division realizes that existing FBI security policies should be carefully reexamined to ensure their accuracy and understanding and that the effective pursuit of security programs requires their collation into one document.

This manual is a living document. It will be amended as new legal authorities are issued and as security requirements change and will undergo a total review every five years. All consumers are invited to provide the Security Division recommendations on improving this product. This manual addresses both old and new security procedures and takes precedence over other policies in electronic communications or other security documents.

Intended Audience. This manual applies to FBI employees, contractors working in FBI facilities, detailees, and any other person assigned to or detailed to the FBI. It also applies, where appropriate, to members of state and local law enforcement personnel assigned to FBI Joint Task Forces and Joint Terrorism Task Forces, and any other persons assigned to work in an FBI-controlled facility. It also applies to FBI information security systems.

The FBI security program is multifaceted and requires the willingness of all FBI employees and others working in FBI facilities to follow established security policy to ensure a successful security program designed to protect FBI critical resources.
Key Terms and Acronyms

(See Appendix A for a complete listing of key security terms.)

**Classified Information**: Information that has been determined (pursuant to EO 12958, as amended, or any predecessor order) to require protection against unauthorized disclosure and is marked to indicate its classified status when in digital or hard copy form. The levels TOP SECRET, SECRET, and CONFIDENTIAL are used to mark and designate such information.

**Closed Storage Secure Area**: An approved space in which all classified and sensitive information (to include, paper, hard drives, crypto keys, etc) must be secured in a GSA-approved security container when the material is not in use and the space is not occupied.

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

**Derivative Classification**: The incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that applies to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

**Intelligence Sources and Methods**: Comprised of the classified sources and methods the DNI protects under Section 102 of the National Security Act of 1947 and Executive Order 12333.

**Need-to-Know**: A determination by an authorized holder of classified or sensitive information that access to specific material in their possession is required by another person to perform a specific and authorized function to carry out a national task.

**Open Storage Secure Area**: An approved space for the open storage of material up to and including the Secret collateral level.

**Original Classification**: An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

**Password**: A private alpha-numeric character string used to authenticate an identity or to gain access.

**Sensitive Compartmented Information (SCI)**: Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.
### Acronyms

(See Appendix B for a complete listing of acronyms.)

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD</td>
<td>Assistant Director</td>
</tr>
<tr>
<td>BMS</td>
<td>Balanced Magnetic Switch</td>
</tr>
<tr>
<td>C&amp;A</td>
<td>Certification and Accreditation</td>
</tr>
<tr>
<td>COOP</td>
<td>Continuity of Operation Plan</td>
</tr>
<tr>
<td>CSA</td>
<td>Cognizant Security Authority</td>
</tr>
<tr>
<td>CSO</td>
<td>Chief Security Officer</td>
</tr>
<tr>
<td>CUA</td>
<td>Co-Utilization agreement</td>
</tr>
<tr>
<td>DAA</td>
<td>Designated Approving Authority</td>
</tr>
<tr>
<td>DCI</td>
<td>Director of Central Intelligence</td>
</tr>
<tr>
<td>DCID</td>
<td>Director of Central Intelligence Directive</td>
</tr>
<tr>
<td>DNI</td>
<td>Director of National Intelligence</td>
</tr>
<tr>
<td>DOJ</td>
<td>Department of Justice</td>
</tr>
<tr>
<td>DIDO</td>
<td>Designated Intelligence Disclosure Officer</td>
</tr>
<tr>
<td>EO</td>
<td>Executive Order</td>
</tr>
<tr>
<td>FFC</td>
<td>Fixed Facility Checklist</td>
</tr>
<tr>
<td>FGI</td>
<td>Foreign Government Information</td>
</tr>
<tr>
<td>FSI</td>
<td>Foreign Service Institute</td>
</tr>
<tr>
<td>FISMA</td>
<td>Federal Information Security Management Act</td>
</tr>
<tr>
<td>FOUO</td>
<td>For Official Use Only</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>ISSM</td>
<td>Information System Security Manager</td>
</tr>
<tr>
<td>ISSO</td>
<td>Information System Security Officer</td>
</tr>
<tr>
<td>JTF</td>
<td>Joint Task Force</td>
</tr>
<tr>
<td>JTTTF</td>
<td>Joint Terrorism Task Force</td>
</tr>
<tr>
<td>NdA</td>
<td>Non-disclosure Agreement</td>
</tr>
<tr>
<td>OEP</td>
<td>Occupant Emergency Plan</td>
</tr>
<tr>
<td>PED</td>
<td>Portable Electronic Device</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PR</td>
<td>Periodic Reinvestigation</td>
</tr>
<tr>
<td>SAC</td>
<td>Special Agent in Charge</td>
</tr>
<tr>
<td>SACS</td>
<td>Security Access Control System</td>
</tr>
<tr>
<td>SCI</td>
<td>Sensitive Compartmented Information</td>
</tr>
<tr>
<td>SCIF</td>
<td>Sensitive Compartmented Information Facility</td>
</tr>
<tr>
<td>SIP</td>
<td>Security Incident Program</td>
</tr>
<tr>
<td>SOIC</td>
<td>Senior Official of the Intelligence Community</td>
</tr>
</tbody>
</table>

---

3
STE: Secure Telephone Equipment
STU: Secure Telephone Unit
Summary of Legal Authorities

(See Appendix C for a complete listing of legal authorities.)


- EO 12148, Federal Emergency Management
- EO 12656, Assignment of Emergency Responsibilities
- EO 12968, Access to Classified Information
- EO 13011, Federal Information Technology, July 16, 1996

- PDD 39, United States Policy on Counterterrorism
- PDD 62, Protections Against Unconventional Threats to the Homeland and Americans Overseas
- PDD 63, Protecting America’s Critical Infrastructures, May 22, 1998

- DCID 6/1, Security Policy for Sensitive Compartmented Information, March 1, 1995
- DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems, June 3, 1999
- DCID 6/6, Security Controls on the Dissemination of Intelligence Information

- DOJ Order 2630.4C, Occupant Emergency Program
- DOJ Order 2640.2E, Information Technology Security

Roles and Functional Responsibilities

1. **Individuals**
   - Comply with the provisions of this manual.

2. **Assistant Director, Security Division**
   The Assistant Director (AD), Security Division, is responsible for
   
   and
   
   the AD, through the Security Division organizational
   structure, will:
3. Assistant Directors and Special Agents in Charge (Division Heads)

Division Heads have overall responsibility for effective implementation of all elements of the FBI Security Program. Division Heads will:

- 
- 

7

UNCLASSIFIED//FOR OFFICIAL USE ONLY
4. Chief Information Officer (CIO)
In addition to the responsibilities in paragraph 3, above, the CIO is the

5. Chief Security Officers (CSO)
The CSO is a full-time assignment responsible for
6. Information System Security Manager (ISSM)

7. Information System Security Officer (ISSO)

8. System Administrator

9. All Supervisors
Policies

1. Security Management

1.1. Purpose
The FBI security program is multifaceted and requires the compliance of all FBI employees and others working in FBI facilities to ensure the protection of FBI people, information, operations, equipment, and facilities. This manual contains

1.2. General
The security policy and procedures set forth in this manual are the standards for

1.3. Risk Management
The FBI security program will be based on risk management principles in order to provide protection without excessive cost in dollars or in the efficient flow of information to those who need it. Risk management is the process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost. The total risk of operating a system is assessed as a combination of the risks associated with all possible threat scenarios. Risk is reduced by countermeasures.
1.4. Dissemination and Disclosure under Emergency Conditions

1.5. Public Declarations

Classified information may not be released to or discussed with the public media.

Declassification of other information will be according
1.6. Foreign Disclosure
The following provisions may not be waived:

- 

1.7. Standard Operating Procedures (SOP)

1.8. Inspections

1.8.1. Security Reviews
EO 12958, as amended, and DOI Security Program Manual require self-reviews of security programs.
1.9. Security Awareness Program

Consistent with the requirements of EO 12958, as amended, and DCID 6/1, Security Policy for Sensitive Compartmented Information, each Division Head will establish a continuing security awareness program that will provide frequent exposure of personnel to security awareness material. The continuing awareness program training methods may include:

- Such a comprehensive effort must meet the varying levels of knowledge, experience, and responsibilities of employees, as well as the specific needs of individual divisions within the FBI.

The security awareness program is divided into three phases: Phase 1
1.9.1. Phase 1 security awareness will include the following:
1.9.2. Phase 2 is the continuing security awareness training and will include at a minimum:

- Periodic reminders of requirements in Phase 1.

1.9.3. Phase 3 of the continuing security awareness program is executed when access to classified information, including SCI, is terminated.

1.9.4. Other Training Requirements

Individuals designated as Original Classification Authorities (OCA), authorized declassification authorities will receive training specific to their assigned duties in such positions.

1.11. Security Coordination Requirement

The Security Division's mission is to integrate security into all FBI business processes to protect FBI people, information, operations equipment, facilities, and operations. This mission is essential in supporting the FBI in meeting its most significant challenges to protect the United States from terrorist attack, foreign intelligence operations, espionage, and cyber-based attacks.

1.12. Off-Site Conferences

Meetings, conferences, training courses, or other such gatherings where classified and/or sensitive information is presented or disseminated present special vulnerabilities to unauthorized disclosure and are limited to appropriately cleared U.S. Government and U.S. contractor facilities. Divisions hosting such off-site conferences will ensure the following:

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
-
1.13. Policy Waivers and Exceptions
1.14. Field Personnel Files
1.15. Lock Combination Procedures

Lock combinations will be known only to
2. Personnel Security

2.1. Purpose
Eff. Date: 04/24/2009

2.2. Policy
Eff. Date: 04/24/2009

2.3. Requirements for Clearance and Access
Eff. Date: 04/24/2009

2.3.1. Need-to-Know
Eff. Date: 04/24/2009

2.3.2. Clearance/Access Eligibility
Eff. Date: 04/24/2009

2.3.2.1. Employees
Eff. Date: 04/24/2009

2.3.2.2. Contractors
Eff. Date: 04/24/2009
2.3.2.3. Consultants
Eff. Date: 04/24/2009

2.3.2.4. Contract Linguists
Eff. Date: 04/24/2009

2.3.2.5. Contract Physicians
Eff. Date: 04/24/2009

2.3.2.6. Joint Task Force (JTF)/Joint Terrorism Task Force (JTTF) Members
Eff. Date: 04/24/2009

2.3.3. JTF Security Investigations
Eff. Date: 04/24/2009

2.3.4. Security Clauses for Joint Task Force Memorandum of Understanding
Eff. Date: 04/24/2009

2.3.5. Classified Information Procedures Act (CIPA)
Eff. Date: 04/24/2009

2.3.6. Foreign Intelligence Surveillance Act (FISA) Personnel
Eff. Date: 04/24/2009
2.3.7. **FISA Emergency Circumstances**

Eff. Date: 04/24/2009

2.3.8. **Legislative and Judicial Access**

Eff. Date: 04/24/2009

2.3.9. **Others – Access to National Security Information**

Eff. Date: 04/24/2009

2.4. **Personnel Security Interviews**

Eff. Date: 04/24/2009

2.5. **Non Disclosure Agreement**

Eff. Date: 04/24/2009

2.6. **Indoctrination for Access**

Eff. Date: 04/24/2009

2.7. **Reciprocity**
An employee with an existing security clearance who transfers to or changes employment status with the FBI (e.g. contractor to government or government to government) is eligible for a security clearance at the same or lower level at the FBI without additional or duplicative adjudication, investigation, or reinvestigation, unless there is substantial information that the individual will not meet the adjudication standards. The FBI abides by the reciprocity provisions as established by EO 12968.
2.8. One Time Access

2.9. Interim Clearance
The FBI abides by the provisions for interim clearances as established by EO 12968 and the provisions for temporary SCI access as established by DCID 6/4.

2.10. Inadvertent Disclosure

2.11. Denial or Revocation of Clearance/Access

2.11.1. Denial Procedures
Applicants and employees who are determined not to meet the standards for access to classified information must be:

- Provided with a comprehensive and detailed written explanation of the basis for that decision as the national security interests of the U.S. and other applicable law permit and informed of their right to be represented by counsel or other representative at their own expense;
- Permitted 30 days from the date of the written explanation to request any documents, records, or reports including the entire investigative file upon which a denial or revocation is based; and
- Provided copies of documents requested pursuant to this paragraph within 30 days of the request to the extent such documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), and as the national security interests and other applicable law permit.
2.11.2. Review of Denial or Revocation Determinations

- An applicant or employee may file a written reply and request for review of the determination within 30 days after written notification of the determination or receipt of the copies of the documents requested pursuant to this section, whichever is later.
- An applicant or employee will be provided with a written notice of and reasons for the results of the review, the identity of the deciding authority, and written notice of the right to appeal.

2.11.3. Appeal of Denials or Revocation

- Within 30 days of receipt of a determination under paragraph 2.10.1, the applicant or employee may appeal that determination in writing to the DOJ Access Review Committee (ARC), established under 28 CFR Part 17 § 17.15. The applicant or employee may request an opportunity to appear personally before the ARC and to present relevant documents, materials, and information.
- An applicant or employee may be represented in any such appeal by an attorney or other representative of his or her choice, at his or her expense. Nothing in this section will be construed as requiring the DOJ to grant such attorney or other representative eligibility for access to classified information, or to disclose to such attorney or representative, or permit the applicant or employee to disclose to such attorney or representative, classified information.
- A determination of eligibility for access to classified information by the ARC is a discretionary security decision. Decisions of the ARC will be in writing and will be made as expeditiously as possible. Access will be granted only where facts and circumstances indicate that access to classified information is clearly consistent with the national security interest of the U.S., and any doubt will be resolved in favor of the national security.
- The applicant or employee will have an opportunity to present relevant information in writing or, if the applicant or employee appears personally, in person. Any such written submissions will be made part of the applicant’s or employee’s security record and, as the national security interests of the U.S. and other applicable law permit, will also be provided to the applicant or employee. Any personal presentations will be, to the extent consistent with the national security and other applicable law, in the presence of the applicant or employee.

2.12. Clearance Passage
2.13. Sensitive Compartmented Information (SCI) Access
Eff. Date: 10/06/2010

2.14. Debrief from SCI Accesses and Clearances
Eff. Date: 10/06/2010

2.15. Outside Indoctrination Assistance
Eff. Date: 10/06/2010
2.16. Reinvestigations
Eff. Date: 04/23/2009

2.17. Exit Interviews
Eff. Date: 04/24/2009

2.18. Continuing Clearance for Retiring FBI Officials/Personnel
Effective Date: 09/23/2009

2.19. Outside Activities
• Security Division Authorization.
2.20. Cohabitant/Roommate
Eff. Date: 10/22/2010

2.21. Change in Marital Status
2.22. Official Foreign Travel


Eff. Date: 10/20/2010

2.23. Unofficial Foreign Travel

2.23.1. Travel to Mexico and Canada

2.23.2. Travel to border countries

2.23.3. Travel to Hazardous Locations
2.24. Foreign Contacts

2.24.1. Official Contact with Foreign Government Representatives

2.24.2. Reportable Contact

2.24.3. Unofficial Contact with Foreign Nationals

2.24.4. Adoption of a Foreign National
2.24.5. Failure to Report

2.24.6. Contact with Foreign Nationals Records Checks

2.25. Financial Disclosure

Eff. Date: 01/06/2009

2.26. Polygraph Program
Each polygraph interview and examination will be conducted and reported with high professional, ethical, and technical standards. Observation of polygraph examinations or recordings thereof will be limited to that necessary for supervision, quality control, training, investigation, inspection, language interpretation, legal representation, and administrative or judicial action.

- Applicants for FBI employment will first undergo a Personnel Security Interview followed by a pre-employment polygraph examination.
2.26.1. Authorization for Conducting Examinations
The Director is the approving authority for polygraph examinations and hereby delegates such authority to:

- **Security Matters:**
- **Administrative Matters:**
- **Non-Administrative Matters:**

2.26.2. Factors to be Considered in Authorizing Examinations
2.26.3. Routine and Periodic Polygraph Examinations for Bureau Employees

2.26.4. Polygraph Examinations of FBI Employees Who Are Required to Submit to an Employee Interview Regarding Security Matters

2.26.5. Use of the Results of Polygraph Examinations Regarding Security Matters
2.26.6. Polygraph Examinations of FBI Employees Regarding Administrative Matters

When approved, polygraph examinations may be conducted to resolve an issue during the investigative phase of a disciplinary matter. The examination must be conducted in accordance with Bureau regulations for employee interviews.
The following requirements must be satisfied when an employee is ordered to submit to a polygraph examination:

- If the examinee is suffering from any current illness or physical condition, consideration should be given to rescheduling the examination.
- If it is determined that an examinee is pregnant, a physician’s waiver should be obtained prior to conducting a polygraph examination.

2.26.7. Use of the Results of Polygraph Examinations Regarding Administrative Matters

2.26.8. Polygraph Examination Procedures

2.26.8.1. Examinee’s Mental and Physical Fitness

Due to the nature of the polygraph examination the following guidelines apply:

- If the examinee is suffering from any current illness or physical condition, consideration should be given to rescheduling the examination.
- If it is determined that an examinee is pregnant, a physician’s waiver should be obtained prior to conducting a polygraph examination.
2.26.8.2. Examinee’s Ability to Respond

- Polygraph examinations will not be conducted if, in the opinion of the examiner, any of the following inhibit the individual’s ability to respond or otherwise cause the individual to be an unfit candidate for examination:
  - It is apparent that the examinee is mentally or physically fatigued.
  - The examinee is unduly emotionally upset, intoxicated, or adversely under the influence of a sedative, stimulant, or tranquilizer.
  - The examinee is known to be addicted to narcotics.
  - The examinee is known to have a mental disorder which causes the examinee to lose contact with reality or which could reasonably result in the examinee becoming violent during a test.
  - The examinee is experiencing physical discomfort of significant magnitude or appears to possess disabilities or defects which, in themselves, might cause abnormal physiological reactions.
  - Should the examiner or examinee have any doubt concerning the above conditions, the matter should be referred to the FBIHQ Polygraph Unit for determination and appropriate action. An examiner will not attempt to make a psychiatric or physical diagnosis of an examinee.
  - If an examiner has any doubt concerning the ability of an examinee to safely undergo an examination, a statement from the examinee’s physician must be obtained before proceeding with the test.

2.26.8.3. Pretest Interview

During the pretest interview the examiner will advise the examinee of the following:

- Of his/her rights, if appropriate, in accordance with the “self-incrimination clause” of the Fifth Amendment to the Constitution and that an attorney may be obtained and consulted.
- That the examination will be conducted only with the examinee’s prior consent.
Of the characteristics and nature of the polygraph instrument, the procedures to be followed during the examination and all the questions to be asked during the testing phase of the examination.

Whether the area in which the examination is to be conducted contains a 2-way mirror or other observation device, and whether the conversation during the examination will be monitored in whole or in part by any means.

2.26.8.4. Execution of Forms

An appropriate consent or agreement form will be executed during the pre-test interview before the examination. Should the examinee agree to be examined, but refuse to sign the consent or agreement form, that fact should be noted on the form by the examiner and witnessed by one other person. FD-328, Consent to Interview With Polygraph and FD-328a, Employee Agreement To Interview With Polygraph in Connection With An Administrative Interview will be used.

3. Visitor Control

Eff. Date: 08/03/2009

4. Foreign National Access to FBI Facilities

4.1. Purpose

Eff. Date: 05/25/2009

4.2. Policy

Eff. Date: 05/25/2009

4.3. Definitions

Eff. Date: 05/25/2009
4.4. Responsibilities

4.4.1. Security Division
Eff. Date: 05/25/2009

4.4.2. HQ Divisions and Field Offices
Eff. Date: 05/25/2009

4.4.3. Office of International Operations, International Visits and Protocol Unit (IVPU), and Field Office CSO
Eff. Date: 05/25/2009

4.4.4. Chief Security Officer
Eff. Date: 05/25/2009

4.5. Disclosure or Release of Intelligence Information
Eff. Date: 05/25/2009

4.6. Escort Requirement
Eff. Date: 05/25/2009

4.7. Unexpected Foreign National Visitors
Eff. Date: 05/25/2009
4.8. VIP Foreign National Visitors
Eff. Date: 05/25/2009

4.9. Hosted Visits
Eff. Date: 05/25/2009

4.10. Foreign National Access to SCIFs
Eff. Date: 05/25/2009

4.11. Foreign National Access to Information Systems and Telephones

4.12. Foreign Nationals with a Security Detail
Eff. Date: 05/25/2009

4.13. Vendors
Eff. Date: 05/25/2009

Eff. Date: 05/25/2009

4.15. Foreign Integrated Person (FIP)
Eff. Date: 05/25/2009

42
4.15.1. Memorandum of Agreement (MOA)
Eff. Date: 05/25/2009

4.15.2. Security Plan
Eff. Date: 05/25/2009

4.15.3. Position Description
Eff. Date: 05/25/2009

4.15.4. Administrative and Operational Control
Eff. Date: 05/25/2009

4.15.5. Supervisor Responsibilities
Eff. Date: 05/25/2009

5. National Security Information

5.1. Purpose
To establish standards for classifying, safeguarding, and declassifying FBI national security information.

5.2. Policy
- All FBI personnel and all persons to whom this manual applies are personally and individually responsible for providing proper protection to classified information under their custody and control.
- Information will be classified only if its meets the standards for classification and its disclosure reasonably could be expected to cause damage to national security according to Executive Order (EO) 12958, Classified National Security Information Act, as amended.
The author or drafter of a document is responsible for complying with established security classification guidance and for properly applying that guidance to a document, regardless of the media, including all markings required for its protection, control, and dissemination. A higher level official through or to whom a document or other material passes for signature or approval becomes jointly responsible with the classifier for the classification assigned.

5.3. Definitions

- **Classification Block.** Information on the face of a classified document which conveys the classification authority, reason for classification, and declassification instructions for classification decisions.

- **Classification Guide.** A documentary form of classification guidance issued by an Original Classification Authority (OCA) that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

- **Classified National Security Information or Classified Information.** Information that has been determined pursuant to EO 12958, as amended, or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

- **Declassification.** The authorized change in the status of information from classified to unclassified information.

- **Derivative Classification.** The incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that applies to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

- **Exemption Codes.** A combination of the letter “X” and a number, one through eight, which referred to information exempt from declassification within 10 years. These codes are obsolete.

- **Original Classification.** An initial determination by an OCA that information requires, in the interest of the national security, protection against unauthorized disclosure.

- **Original Classification Authority (OCA).** Within the FBI, an individual authorized in writing by the Assistant Director, Security Division (SecD), to classify information in the first instance.

- **Portion Marking.** Marking parts of a document, such as a paragraph, sub-paragraph, title, subject, graphic, table or appendix, to indicate the highest level of classified information contained in the portion.
• Safeguarding. The measures and controls prescribed to protect classified information.

• Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence (DNI).

• Working Papers. Documents or materials, regardless of the media, which are expected to be revised prior to the preparation of a finished product for dissemination or retention.

5.4. Classification and Declassification Authorities

5.4.1. Original Classification Authority (OCA)
An OCA is an official authorized in writing by the Assistant Director, Security Division, to make classification decisions in the first instance.

• Delegations of OCA. Delegations of OCA are limited to the minimum number required for efficient administration and to those officials who have a demonstrable and continuing need to exercise it. Designation of an OCA is based on the position or title, not the individual, and may not be further delegated. When an OCA is absent, the person designated to act in the official’s absence may exercise classification authority.

• OCA Responsibilities. OCAs are responsible for adhering to the standards for classification according to EO 12958, as amended, (see Item 12, Standards for Classification, in Appendix D: Hyperlinks) and for developing security classification guides for the program or system for which they hold original classification authority.

• OCA Training Requirement. OCAs will receive training in original classification. Such training will include instruction on the proper safeguarding of classified information and of the criminal, civil, and administrative sanctions that may be brought against an individual who fails to protect classified information from unauthorized disclosure.

5.4.2. Derivative Classifiers
All FBI personnel with the appropriate clearances and accesses are authorized to derivatively classify information. Derivative classifiers will observe and respect source document classification markings and carry forward to any newly created documents the pertinent markings and safeguarding requirements.
5.4.3. Declassification Authority
Information may be declassified prior to the established declassification date or event by an original classification authority with jurisdiction over the information as defined in EO 12958, as amended. Classified information declassified without proper authority remains classified.

5.5. Compilation
In unusual circumstances, compilation of elements of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that qualifies for classification and is not otherwise revealed by the individual portions of information. Classification by compilation also includes raising the overall classification of a document to a higher level than its individual portions. Classification by compilation will be based on security a classification guide instruction that describes the compilation of elements of information at a specified classification level or a determination of an OCA.

5.6. Marking Classified Information

5.6.1. Classification Levels
Information may be classified at one of the following three levels: Top Secret, Secret, or Confidential. Except as provided by statute, no other terms will be used to identify United States classified information. Information may be classified originally or derivatively.

5.6.2. Original Classification
Only an OCA, authorized in writing, may originally classify information. OCAs must identify the classification authority, the reason for classification, and provide declassification instructions. This information is provided on the Classified By, Reason, and Declassify On lines in the classification block placed on the face of each originally classified document, regardless of the media.

5.6.3. Classification Authority

5.6.4. Reason for Classification
The OCA will identify the reason(s) for the decision to classify. In no case will information be classified in order to conceal violations of law, inefficiency, or administrative error; prevent embarrassment to a person, organization, or agency; restrain competition; or prevent or delay the release of information that does not require protection in the interest of the national security. The OCA will identify the reason for classification by identifying Section 1.4 of the Order plus the letter that corresponds to
5.6.5. Declassification Instructions

Exemption categories X1 through X8 are obsolete markings. When determining the duration of classification for information originally classified under the Order, the OCA will attempt to set a date or event that corresponds to the lapse of the information’s national security sensitivity. An OCA will attempt to determine a declassification date in the following sequence: A date or event less than 10 years from the date of original classification; a date or event 10 years from the date of original classification; or a date or event not to exceed 25 years from the date of original classification. When information pertains to the identity of a confidential human source or a human intelligence source, the information will be marked 25X1-human. This marking denotes that the information is not subject to automatic declassification.
5.6.6. Derivative Classification

The classification block of a derivatively classified document consists of two elements: the “Derived From” line and the “Declassify On” line. The derivative classifier will identify the source document or classification guide and the agency of origin on the “Derived From” line and provide declassification instructions on the “Declassify On” line. (Note: Only an OCA may use “Classified By.”)

5.6.6.1. Identification of Derivative Classification Source

- **Identification of Single Source Document.** The derivative classifier will identify the source document or the classification guide, the agency of origin, and the date of the source or guide on the “Derived From” line. If the source document is itself marked with “Multiple Sources,” the derivative classifier will quote the source document on the “Derived From” line rather than the term “Multiple Sources.”

- **Classification Guide as a Source.** Derivative classifiers will follow the declassification instructions in the subject matter classification guide. When a classification guide carries instructions based on exemption codes (e.g., X1), the declassification date will be 25 years from the date of the new document. For example, a derivative classifier prepares a document dated February 24, 2004; the classification guide provides declassification guidance as X1: the document dated February 24, 2004, would reflect a “Declassify On” date of February 24, 2029.

- **Multiple Sources.** If the information is derivatively classified from more than one source, the “Derived From” line will show “Multiple Sources.” The derivative classifier will maintain a listing of all sources with the record or file copy of the derivatively classified document.

5.6.7. Declassification Instructions

The derivative classifier will carry forward the instructions on the “Declassify On” line from the source document or the duration instruction from the classification guide.

- **Multiple Sources.** When extracting classified information from more than one source or more than one element of a classification guide, carry forward the longest duration of any of the sources.
5.6.8. **Classification by Compilation**
Documents containing information classified by compilation will be marked as follows:

- If portions, standing alone, are unclassified, but the document is classified by compilation, mark the portions "(U)" and the document and pages with the overall classification of the compilation.
- If individual portions are classified at one level but the compilation is a higher classification, mark each portion with its own classification, and mark the document and pages with the classification of the compilation.
- An explanation of the basis for classification by compilation will be placed on the face of the document or included in introductory text.

5.6.9. **Foreign Government Material**
5.7. Classification Prohibitions and Limitations

In no case will information be classified in order to conceal violations of law, inefficiency, or administrative error; prevent embarrassment to a person, organization, or agency; restrain competition; or prevent or delay the release of information that does not require protection in the interest of the national security.

5.8. Classification Markings

FBI documents will be marked using the Intelligence Community marking format as established by the Director of National Intelligence (DNI). This system commonly referred to as the “CAPCO (Controlled Access Program Coordination Office) markings,” uses a uniform list of security classification and control markings authorized for all dissemination of classified information by components of the Intelligence Community.

5.8.1. Portion Marking

Classifiers will mark each portion of a classified document to indicate its classification level and dissemination controls. Portions will be marked at the beginning of the portion.

5.8.2. Overall Classification

Classifiers will conspicuously mark classified documents with the highest level of classified information in the document. Place the overall classification marking (also referred to as the “header and footer”) at the top and bottom of the outside of the front cover, the title page, on the first page, and on the outside of the back cover. Mark each interior page with the overall classification marking. As an option, classifiers may mark each interior page with the highest classification of information contained on the page, including the designation “Unclassified,” where applicable. Correspondence and other documents without cover pages do not require marking on the back of the last page.

5.9. Marking Specialized Items
5.9.1. Information Systems Storage Media


Eff. Date: 08/04/2009

5.9.2. Photographic Media

- Label photography in roll, flat, or other form with its classification, caveats, and dissemination controls. For film in roll form, place the label on the end of the spool flange, on the side of the spool container, and on the container cover (if any). If the container and its cover are transparent, no label is needed if the flange label is visible through the container. The roll film will include head and tail sequences giving all security markings applicable to its contents.

- Mark positive film flats or slides with individual internal markings showing the classification and SCI and other control markings. Label the front and back of frames for slides and view graphs with the classification and required markings which may be abbreviated if necessary to fit the space provided. When feasible, photographically burn the classification and caveats into the print, slide, or image itself.

5.9.3. Video Tapes/Movie Film

Each video tape/movie film will contain the classification and control information at the beginning and end of the movie. Label video cassettes/tape reels and containers to show the title, security classification, caveats, and dissemination control markings.

5.9.4. Graphic Arts Material

Mark visual aids, maps, artwork, blueprints, and such other material with the classification and dissemination controls under the legend, title block, or scale, and at the top and bottom in such a manner as to be reproduced on all copies.

5.9.5. Teletypes

Teletypes are marked with the classification level and handling caveats or dissemination controls preceding the text on the first page and at the top of each succeeding page. The abbreviations "CLASS" for "Classified by," "RSN" for "Reason," "DECL" for "Declassify on," and "DERV" for "Derived from," will be used at the end of teletype messages.
5.10. **Cover Sheets**

Cover sheets assist in protecting classified information from unauthorized disclosure and remind the holder of the material about the sensitivity of the information.

- Cover sheets, conveying the highest classification of information in the document, will be attached to the face of each classified document regardless of the authorized facility in which it is used. Classified material, such as publications or notebooks, which carry a cover page indicating the classification of the material, do not require an additional cover sheet as long as the cover page does not convey classified information.

- Cover sheets are required when transmitting documents via the FBI messenger system and when transmitting the material outside FBI facilities.

- Standard Forms 703, 704, and 705 for Top Secret, Secret, and Confidential, respectively, will be used for collateral classified documents. Color-coded SCI cover sheets, specific to the SCI compartments, are available on the Security Division Web page (see item 16, Classified documents coversheets, in Appendix D: Hyperlinks).

- Coversheets should be removed before filing the material in an authorized storage container. Folders will be marked to show the highest classification of materials stored in the folder. Folders may be marked by stamping, labeling, or other method that conspicuously shows the classification level.

5.11. **Classification Challenges**

Authorized holders of classified information, who, in good faith, believe that specific information is improperly classified, should informally attempt to resolve the issue with the author of the document or OCA. If not resolved, authorized holders may formally challenge the classification in writing. The information will be protected at the classification level initially assigned until the challenge is resolved. No retribution may be taken against any authorized holders bringing such a challenge in good faith.

5.11.1. **Other Government Agency Information**

Challenges to information classified by other government agencies will be addressed to the organization and coordinated with the APU. The letter will give a description of the information being challenged and state the reason the information is believed to be improperly classified. If the FBI does not agree with the decision of the other government agency, the decision can be appealed to the Interagency Security Classification Appeals Panel through DOJ. APU will provide assistance in the appeals process. The decision of the Appeals Panel is final.

5.11.2. **FBI Information**
5.11.3. **Challenges from Other Government Agencies**

Formal challenges to FBI classification decisions will be referred to the DOJ Department Review Committee according to DOJ “Security Program Operating Manual.”

5.11.4. **Materials with Different Classification levels or Declassification Dates**

When classified material consists of two or more items of information which bear different classification levels or declassification dates, the following guidelines apply: Materials containing different levels of classified information must be classified at the highest level of the highest classified component. Materials containing different declassification dates must be marked with the most distant declassification date.

5.11.5. **Materials Classified Under Prior Orders**

When incorporating FBI information classified under previous Executive Orders into a new document and no specific declassification date was indicated thereon, or if it was marked “indefinite,” or “OADR,” the declassification date will be based on the National Security Information Security Classification Guide. The information must continue to meet the standards for classification under the EO 12958, as amended. It is possible that the “declassification date” may have passed, and the information may be determined to be unclassified.

5.11.6. **Atomic Energy Material Markings**

5.12. **Security Classification Guides**
5.13. Classifications Guidance
Classification guidance for FBI information is provided in classification guides posted on the Security Division Web site.


5.15. Foreign Government Information (FGI)

5.15.1. Top Secret FGI

5.15.2. Secret FGI
5.15.3. Confidential FGI

5.16. Restricted and Other FGI Provided in Confidence
5.17. Classification of Intelligence Activities

5.18. Transmittal documents
An EC, letter, memorandum, or other correspondence which transmits classified information as enclosures is referred to as a letter of transmittal. A transmittal letter may be classified or unclassified. When a letter of transmittal is separated from its enclosure, remark the letter according to the notation on the letter.

5.18.1. Classified Transmittal Letters
If the transmittal letter itself contains classified information, mark the letter with the highest classification, caveats, and dissemination control markings of the letter and the...
5.18.2. Unclassified Transmittal Letters
If a transmittal letter itself is unclassified but has one or more classified enclosures, mark the letter with the highest classification caveats, and control markings of the enclosures. Unclassified transmittal letters do not require portion marking.

5.19. Working Papers
Drafters of working papers will date them when created, mark with the overall classification, protect at that level, and destroy when no longer needed. When released by the originator outside the originating activity for other than coordination purposes, retained more than 180 days from date of origin, or filed permanently, working papers will be controlled and marked in the same manner as a finished classified document. Working papers may not be cited as a derivative classification source.

5.20. Marking Old FBI Classified Documents
All pre-1974 documents in FBI file classifications, other than those in the FBI file classifications in the appendix to the Declassification Guide, will be bulk declassified without review. These documents will either be destroyed, in accordance with Records Retention Schedules, or sent to the National Archives and Records Administration for historical purposes. NARA will conduct a classification review of these documents, in accordance with Intelligence Community Standards, prior to their release or review by the public. Those FBI file classifications listed in the appendix to the Declassification Guide will be reviewed since they are recommended for exemption from the automatic declassification provisions of the EO.

5.21. Facsimile Control Procedures
Eff. Date: 07/06/2010

5.22. Storage of Classified Information
- **Sensitive Compartmented Information.** Regardless of classification level, SCI will only be stored in SCIFs. Storing SCI in SCIFs accredited for open storage means the material, with an appropriate cover sheet, does not require further storage protection. SCI in a SCIF accredited for closed storage must be stored at the end of duty hours in a GSA-approved security container.

- **Collateral Top Secret, Secret, and Confidential.** In open storage secure areas, Secret and Confidential materials do not require further storage in GSA-approved security containers. When not in use, Top Secret materials will be stored in a GSA-approved security container. In closed storage secure areas, classified and sensitive materials will be stored in a GSA-approved security container when the materials are not in use. In open and closed storage secure areas, Top Secret will be stored separately from Secret and Confidential materials.

5.23. Removal of Classified Materials to Residence

UNCLASSIFIED//FOR OFFICIAL USE ONLY
5.24. Transmission and Transportation
Classified information will be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipient. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information in accordance with this manual.

5.24.1. Secret Enclave (formerly known as FBINET)

5.24.2. Top Secret Information

5.24.3. Secret Information
Secret information will be transmitted by:
- Any of the means approved for the transmission of Top Secret information.
5.24.4. Confidential Information
Confidential information will be transmitted by:

- Any of the means approved for the transmission of Secret information.

5.24.5. Transmission within Field Offices

5.24.6. Transmission within FBI Headquarters

5.24.7. Transmission to Foreign Governments

5.25. Preparation of Material for Transmission
Classified material will be prepared for shipment, packaged, and sealed in ways that minimize risk of accidental exposure or undetected deliberate compromise.

5.25.1. Packaging Classified Material
5.25.2. Addressing Classified Material

5.26. Hand-Carrying Classified Material

5.26.1. General Requirements
5.26.2. Approving Authorities

5.26.3. Courier Card/Letter
5.26.4. Hand-carrying Classified Material on Commercial Aircraft outside the United States
6. Destruction of Classified and Sensitive Material

6.1. Purpose

6.2. Policy

6.3. Definitions

- **Clearing.** Removal of data from an information storage device, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (e.g., keyboard strokes); however, the data may be reconstructed using laboratory methods. Cleared media may be reused at the same classification level or at a higher level. Overwriting is one method of clearing.

- **Degaussing.** A procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing.

- **Erasure.** Process intended to render magnetically stored information irretrievable by normal means.

- **Magnetic Remanence.** Magnetic representation of residual information remaining on a magnetic medium after the medium has been cleared. See clearing.

- **Purging.** Rendering stored information unrecoverable. See sanitize.

- **Remanence.** Residual information remaining on storage media after clearing. See magnetic remanence and clearing.

- **Residue.** Data left in storage after information processing operations are complete, but before degaussing or overwriting has taken place.
Sanitize. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs. See purging.

6.4. Destruction Methods
To preclude recognition or reconstruction of classified materials, the following destruction methods are established for specific types of classified material. Destruction of material not addressed in this policy will be coordinated with the Security Equipment Program Manager.

6.4.1. Paper

6.4.2. Flexible Magnetic Storage Media
6.4.3. Magnetic Tapes

6.4.4. Rigid Magnetic Storage Media

- Sealed Disk Drives.

- Procedures for Sanitization by Bulk Erasure.

- Disposal of Sanitized Sealed Disks

6.4.5. Removable Disk Packs
6.4.6. Magnetic Memory Devices

6.4.7. Optical Storage Media

6.4.8. Volatile and Non-Volatile Memory
6.4.9. Microforms

6.4.10. Printer Platens and Ribbons

6.4.11. Laser Printer Drums, Belts and Cartridges

6.4.12. Copiers

6.4.13. Computers
6.4.14. Communications Security

6.5. Destruction of Top Secret and SCI Material

6.6. Official Trash

6.7. Responsibilities of Division Security Officers
7. Security Access Control System Badge Policy.


Eff. Date: 08/03/2009

8. Physical and Technical Security — Sensitive Compartmented Information Facility (SCIF)

8.1. Purpose

8.2. Policy
8.3. SCIF Accreditation Requirements

8.3.1. Concept and Preconstruction Approval

8.3.2. Construction Requirements and Specifications
8.3.2.2. Suspended Ceilings

8.3.2.3. Windows
8.3.2.9. Primary Entrance Door

8.3.2.10. Secondary Entrance Doors
8.3.2.11. SCIF Emergency Exit Door

- 
- 
- 
- 
- 
- 

8.3.3. Alarm Coverage

8.3.4. Technical Security Countermeasure Requirements (TSCM)
8.3.5. Submitting Accreditation Package

9.4. Classification Guidance

8.5. Re-Accreditation
8.6. Changes to Security Posture

8.7. Modifications/Changes

8.8. Withdrawal of Accreditation

8.9. Occupant Emergency Plan (OEP)
8.10. Co-utilization
8.11. Access Control

8.11.1. Access Rosters

8.11.2. Visitor Log

8.12. Photography In/Around SCIFs

8.13. Alarm Response Time
9. Physical and Technical Security — Open Storage Secure Areas

9.1. Purpose

9.2. Policy

9.3. Construction Requirements and Specifications

9.3.1. Perimeter Walls
9.3.2. Doors

9.3.2.1. Primary Entrance Door

9.3.2.2. Secondary Entrance Doors

9.3.2.3. Emergency Egress Doors
9.3.3. Intrusion Detection Systems (IDS)

9.3.4. Access Control System
9.3.5. Closed Circuit Television (CCTV) - For New Facilities

9.3.6. Windows

9.3.7. Ductwork
9.3.8. Sound Attenuation

9.3.9. Technical Security Countermeasures (TSCM) Inspection

9.3.10. Secure Area Approval Process
9.4. Security Procedures

9.5. Occupant Emergency Plans (OEP)
9.6. Emergency Destruction Identification

9.7. Security Equipment Room or Closet


10.1. Purpose

10.2. Policy

•

•

•
10.3. Closed Storage Area Requirements

10.3.1. Perimeter Walls

10.3.2. Perimeter Doors
10.3.4. Windows
10.3.5. Sound Attenuation

10.4. Secure Area Approval Process

10.5. Access Control

10.6. Security Procedures
10.7. Occupant Emergency Plans (OEP)
10.8. Security Equipment Room or Closet

11. Firearms in FBI-Controlled Spaces

11.1. FBI Employees
11.2. Non-FBI Employees

12. Entry/Exit Inspection Program

12.1. Purpose

12.2. Policy

12.3. Extent of Inspections

•

•
12.4. Seized Items

- Receipts will be given for all seized items. Seized items found not to pose problems will be returned to their rightful owners expeditiously.

12.5. Consequences of Refusals to Participate in Program

12.6. Persons Carrying Out Policy and Training
12.7. Efforts To Be Taken To Avoid Inconvenience.

12.8. Notice of Subject to Searches

12.9. Magnetometer (Metal Detector) Screening

12.10. X-Ray Screening.


14. Computerized Telephone Switch for Newly Constructed FBI Facilities
15. Security Review Requirements for Real Property

15.1. Purpose

15.2. Policy

15.3. Applicability

15.4. Definitions

- **Real Property** facilities either federally-owned or privately-owned and government leased through GSA or by the FBI include, but are not limited to, buildings, office suites, office space, houses, apartments, laboratories, garages, warehouses, hangers, storage areas, and parking lots.

- **Security Systems or Devices.** A group of interacting or single mechanical or electrical elements that provide protection from unauthorized use or entry. Examples of security systems or devices include, but are not limited to, walk-through metal detectors, access control security turnstiles, intrusion detection equipment or systems, access control card reader systems, and vehicle barriers.

15.5. Responsibilities

15.5.1. Security Division
15.5.2. Administrative Services Division/Space Management Unit (SMU)

15.5.3. Planning, Design, and Construction Management Unit (PDCMU)

15.5.4. Chief Security Officer (CSO)

15.6. Procedures

15.6.1. Concept Phase
15.6.2. Construction Phase

15.6.3. Completion of Construction Phase

15.7. GSA Involvement

15.8. FBI as Leasing Agent

16. Acquisition Security

16.1. Purpose

16.2. Policy
16.3. Definitions

- **Classified Contract.** Any contract that will or may require access to classified information.

- **Contractor, Licensee or Grantee (hereinafter “contractor”).** A current, prospective or former contractor, licensee or grantee of a US agency or department.

- **Critical Assets.** Information technology hardware, software, and telecommunications and audiovisual equipment.

- **DD Form 254 (Contract Security Classification Specifications).** Document that provides security classification guidance to a contractor performing on a classified contract. It is a legal document that directs the contractor about the proper protection of classified material released and/or generated under the contract.

- **DSS (DoD’s Defense Security Service).** The Executive Agent for the NISP. DSS inspects and monitors contractors who require or will require access to, or who store or will store classified information. It further determines the eligibility for access to classified information by contractors and their respective employees.

- **Facility Clearance.** An administrative determination that a facility is eligible, from a security viewpoint, for access to NSI of the same or lower classification level as the clearance being granted.

- **Key Management Personnel.** Owners, officers, directors and executive personnel of a vendor.

- **National Interest Determination.** Justification initiated by the Acquisition Security Unit for a company cleared under a Special Security Agreement through the Department of Defense (DoD), NISP, to provide special authorization for the contractor’s access to proscribed information.
16.4. Responsibilities

16.4.1. Acquisition Security Unit (ASU)

16.4.2. Contracting Officer

- 

16.4.3. Contracting Officer Technical Representatives (COTR)

- 

16.4.4. FBI Representative Assigned to CARC

- 

UNCLASSIFIED//FOR OFFICIAL USE ONLY
16.6. Contracts Involving Sensitive But Unclassified and Law Enforcement Sensitive Information
16.7. Intelligence Community Acquisition Risk Center (CARC) Requirements for all Acquisitions
17. Security Incident Program
Eff. Date: 09/23/2009

18. Occupant Emergency Plans

18.1. Purpose

18.2. Policy
- FBI divisions are to protect life and property by maintaining effective OEPs for all occupied facilities.
- In buildings or facilities where the FBI is the prime tenant, the senior FBI official in charge of the FBI resident component, with the assistance of the Division CSO and Safety Officer, will be responsible for the development of the OEP. Where the FBI is not the prime tenant, the senior FBI official in charge will cooperate with the prime tenant to develop an OEP. If the prime tenant fails to develop an adequate OEP, the senior FBI official in charge will develop an independent OEP to ensure the safety and security of FBI personnel, property, information, and operations.
- The primary functions of an OEP are:
18.3. Definitions

- **Command Center.** The location from which emergency operations are directed.
- **Command Center Team.** All emergency operations are directed by the Command Center Team. In large facilities, the Team should include a: Designated Official, Occupant Emergency Coordinator, Floor Team Coordinator, Damage Control Team Coordinator, Medical Coordinator, Administrative Officer, Building Manager, and Physical Security Specialist.
- **Designated Official.** The highest ranking official in a facility or his/her delegate.
- **Occupant Emergency Organization.** Generally consists of a Command Center Team, Floor Teams and a Damage Control Team. Organization members should be provided with visual identifiers such as colored hats or arm bands.
- **Occupant Emergency Plan.** A detailed security programs guidance document denoting the organization and emergency response plans that are required for the evacuation of a facility under emergency conditions.
- **Occupant Emergency Program.** A short-term emergency response program, establishing procedures for safeguarding lives and property during emergencies in particular facilities.
- **Prime Tenant.** An organization with the largest number of employees in a facility.

18.4. Occupant Emergency Plans

The OEP will be in writing and retained in the workplace where it will be available for employees to review. OEPs should be developed with the assistance of an advisory committee. OEPs will establish an Occupant Emergency Organization (OEO) and identify its members and their responsibilities, including who has decision-making authority in any given situation. Establish procedures for notifying the OEO, and when to report to the Command Center. OEO members should know what medical resources are available and how to reach them. OEO members should know under what circumstances they are to report to the Command Center.

- Establish a centrally located and easily accessible Command Center. Provisions should be made for an alternate Command Center in the event that the primary site is
incapacitated. Communications at the Command Center should be adequate, including telephones, portable radios, and messengers to augment the communications system. Employees who have no assigned responsibilities should be excluded from the Command Center. Emergency telephone numbers should be posted in the Command Center and elsewhere, and made readily available, frequently reviewed, and updated.

- Define the responsibility of the owner and security guards.
- Designate rally points which must be at least 200 feet from facilities.
- Establish easy-to-implement procedures for handling serious illnesses, injuries and mechanical entrapments. All occupants should be told how to get first aid. All occupants should know what to do if an emergency is announced, including evacuation procedures, rallying points, routes to them, and shelter-in-place locations. Special procedures should be established for the evacuation of the handicapped.
- Establish firefighting plans which coordinate internal and external resources. Establish fire reporting procedures and ensure all employees know them.
- Establish procedures for reporting a bomb, chemical, biological or radiological threat. Bomb, chemical, biological or radiological device search and disposal responsibilities will be assigned to appropriately trained personnel. A hazard communication program should be established and implemented. Establish an inventory of all hazardous materials used and stored in the facility.
- Ensure floor plans and occupant information is readily available for use by emergency personnel.
- Establish procedures to report the progress of searches and evacuations.
- Establish emergency ventilation system shutdown procedures, and evaluator control plans and shutdown protocols.
- Arrange for emergency repair or restoration of services.
- Establish requirement and plan for training designated emergency response individuals.

18.5. Responsibilities

18.5.1. Assistant Director, Security Division
18.5.2. Assistant Directors and Special Agents in Charge (all divisions).

18.5.3. Chief Security Officer

18.6. OEP Functional Responsibilities

18.6.1. Administrative Officer

18.6.2. Area Monitor
- Directs orderly flow of persons along prescribed evacuation routes.
- Ensures that windows and doors are closed, lights left on and electrical appliances are turned off during fire evacuations.
- Ensures that windows and doors are left open, lights left on and appliances are turned off during bomb threat evacuations.
- Notifies Floor Monitor when area has been completely cleared.
Selects an alternate route in the event that a suspicious item is discovered along the normal evacuation route.

**18.6.3. Building Manager**
- Provides information about the facility and its mechanical systems and reports to the Command Center upon OEP activation.

**18.6.4. Damage Control Coordinator**
- Maintains an emergency call list for utilities and hazardous substances.
- Directs Damage Control Team activities.
- Identifies and maintains plans for building systems, including utilities and shut-off valves, alarm systems and communications equipment.
- Ensures that valves and panels are labeled for easy location.
- Provides technical assessments of physical damage.
- Provides technical information on effected equipment.
- Reports to the Command Center upon OEP activation.

**18.6.5. Designated Official**
- Develops the OEP.
- Trains OEP staff.
- Supervises and expedites the movement of personnel in the event of OEP activation.
- Schedules exercises and drills.
- Establishes working relationships with federal, state and local agencies which might respond to emergencies.
- Reports to the Command Center upon OEP activation.
- Gives the “all-clear” signal at the conclusion of an emergency.
- Account for personnel.

**18.6.6. Elevator Monitor**
- Captures elevators and knows which elevators may be used for evacuating handicapped persons.
- Knows the locations and telephone numbers of handicapped persons.
- Assists handicapped persons from their workplaces and out of facilities.
18.6.7. **Exit Monitor**
- Ensures that exits are open and free of hindrances.
- Denies unauthorized access.
- Directs orderly movement of persons to safety areas.
- Assists in the evacuation of handicapped persons.

18.6.8. **Floor Monitor**
- Ensures that evacuation routes are clearly identified and that office exits are known to occupants.
- Directs the orderly flow of persons during drills and emergencies.
- Maintains a list of disabled persons who may require assistance.
- Ensures that all persons have vacated the floor.
- Reports complete evacuation.

18.6.9. **Floor Team Coordinator**
- Coordinates floor, wing, stairwell, elevator and other monitor activities.
- Reports to the Command Center upon OEP activation.

18.6.10. **Medical Coordinator**
- Identifies available medical emergency services.
- Maintains first aid equipment.
- Arranges CPR, first aid and other paramedical training, and lists persons so trained.
- Provides medical advice on potential health implications.
- Sets up first aid stations, if needed.
- Arranges for ambulance transport, if needed.
- Maintains a list of persons transported to hospitals who require first aid.
- Reports to the Command Center upon OEP activation.

18.6.11. **Occupant Emergency Coordinator**
- Acts for designated official during absences.
- Serves as the principal assistant to the Designated Official, and liaison between the Designated Official and other members of the Command Center Team.
- Establishes evacuation/relocation procedures.
- Maintains building plans.
UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Coordinates training and drills.
- Maintains files on all emergencies.
- Activates the notification system.
- Reports to the Command Center upon OEP activation.
- Develops assessment reports and corrective action plans.
- Account for personnel.

18.6.12. Physical Security Specialist
- Provides advice on security matters.
- Notifies the Command Center of building status and emergency conditions.
- Provides access and notifies the Designated Official of the arrival of local emergency responder.
- Protects the integrity of incident scenes and assists law enforcement and fire authorities in the collection of information.
- Reports to the Command Center upon OEP activation.

18.6.13. Stairwell Monitor
- Controls movement of persons on stairway and inspects stairwell to ensure there are no suspicious items.

18.7. Activation
The Designated Official, or the occupant emergency coordinator in his or her absence, will decide when to activate an OEP. If time permits, advice should be solicited from the GSA building manager, the Federal Protective Service, and other federal, state and local law enforcement agencies. When there is immediate danger to persons and/or property, an evacuation will take place without prior consultation.

Upon activation of continuous sound of fire alarms, all persons in the facility will immediately evacuate and proceed to rally points, or proceed to shelters in place, traveling in a brisk orderly manner, and await further instructions.

18.8. Classified Information
18.9. Shelters-In-Place

Certain incidents such as chemical, biological or radiological releases may make it safer inside a building rather than outside, and require that personnel not be evacuated, but rather ushered to interior declared safe zones until authorities assess the situation.

Shelter in place strategies include providing protective respirators to security and emergency management personnel, providing escape hoods to building occupants, providing weapons of mass destruction training to all personnel, and conducting exercises to validate response plans.

Designated safe zones will stock the following supplies:

- Plastic sheeting, precut to cover doors, vents and windows if windowless locations are not available.
- Duct or masking tape.
- Water.
- Glow sticks or flashlight with extra batteries - one for every ten persons.
- Porta-potties if areas do not have restrooms, if practical or feasible.
- Fans to accommodate the room being sealed and HVAC systems being shut off for four hours or more.
- AM/FM battery-powered radios.
Shelter-in-place procedures include the following:

- All occupants being ordered to report to their assigned zones.
- Monitors ensuring that all windows are closed and locked, and doors closed.
- All air handling equipment being turned off if there is an airborne chemical, biological or radiological threat.
- Sealing all doors, vents and windows.
- Accounting for personnel, using sign-in sheets.
- Monitoring radio broadcasts for emergency messages.
- The posting of signs on the outside of the building advising of the action taken.
- Upon the “all-clear” notice being issued, personnel evacuating the building and gathering at their rally points.

18.10. Training

Training for persons identified in Section 19.5. Responsibilities will be conducted at least annually, and will include duties and responsibilities, the location, use and limitations of fire extinguishers, the locations of rallying points, the locations and use of shelters in place, and the use of emergency equipment, including escape hoods.

Semi-annually, each Designated Official or his/her representative will provide instructions to employees, FBI contractors, and other government agency (OGA) officials.
18.11. Drills
Evacuation and shelter in place drills will be conducted at least annually.

18.12. Plan Reviews, Revisions and Submissions
Plans will be reviewed and updated after each drill, using input from after-action/lessons learned reports. As they are revised, copies of OEPs will be provided to the Security Division, the building manager, the local Regional Office of the Federal Protective Service and DOJ’s Security Officer. All personnel assigned OEP responsibilities will be appointed in writing and copies of said appointments will be forwarded to the Security Division.

18.13. Forms
Forms which may be used in OEPs are to be found in GSA’s “Occupant Emergency Program Guide.”

19. Operations Security

20. Continuity of Operations Plan (COOP)

21. Purpose

21.2. Policy
22. Information Assurance Access Controls
Superseded by Corporate Policy Directive #0256D, titled "Portable Electronic Devices (PEDs)," dated 03/16/2010.
Eff. Date: 03/16/2010

23. Information Assurance System and Information Integrity

23.1. Purpose

23.2. Applicability

23.3. Scope

23.4. KVM (Keyboard, Video and Mouse) Switches Policy
Eff. Date: 05/03/2010

23.5. Prohibition on Playing Personal CDs on Government Systems Policy
Eff. Date: 12/02/2008

23.5.1. Background
Eff. Date: 12/02/2008

23.5.2. Action
24. Information Assurance Identification and Authentication

24.1. Purpose
To establish policy for the use, operation, handling, and control of passwords within FBI-controlled facilities. Identification and authentication form the foundation for information system access control and for user accountability. The most common form of information system identification is the User ID. Generally, there are three means of authenticating User IDs which can be used alone or in combination:

- Something the individual knows such as a password;
- Something the individual possesses such as a smart card or token; and
- Something the individual “is” such as a biometric characteristic.

This policy only addresses the requirements for using password systems for authentication.

24.2. Applicability

24.3. Scope

24.4. Password Systems
24.5. Password Assignment

24.6. Password Management
24.7. Password Protection

24.8. Password Entry
24.9. Public/Private Key Authorization

24.10. Responsibilities

24.11. Information System Security Manager (ISSM)
24.12. Information System Security Officers (ISSOs)

24.13. Chief Security Officer (CSO)

24.15. Enterprise Security Operations Center (ESOC)

24.16. Systems Security and Access Unit (SSAU)

24.17. User

24.18. Information System Requirements

24.18.1. User Identification
24.18.2. Authentication

24.18.3. New Passwords

24.18.4. Inactive Sessions
Eff. Date: 09/17/2007

24.18.5. Password Expiration Notification

24.18.6. Audit Records
"Strong" Password Construction

It is a well-established principle of information system security that strong passwords are an important part of any organization's security posture. Weak passwords can lead to unauthorized access to FBI systems and information. Such access would threaten the mission of the FBI. The following guidelines for strong passwords will ensure that passwords are sufficiently difficult to guess.

Passwords must NOT be:

Passwords must be:
25. Information Assurance Certification and Accreditation
Eff. Date: 10/31/2008

26. Information Assurance Media Protection

27. Information Assurance System and Information Integrity
Eff. Date: 06/10/2008

28. Information Assurance System and Information Integrity

28.1. Purpose

28.2. Policy
28.3. Applicability

28.4. Scope

28.5. Responsibilities

28.5.1. 

* 

*
Appendix A: Definitions

Acceptable Levels of Risk: An authority's determination of the level of potential harm due to loss of information that is acceptable.

Access Authorization: A formal act required to certify that an individual is authorized to have access to SCI.

Access Certification: Temporary certification for access to another organization/SCI facility to accomplish a task, or to attend a meeting or seminar. The parent organization or supporting SSO will certify accesses.

Access Control List: A register of system users and the types of access they are permitted.

Access Control System: A system to identify or admit personnel with properly authorized access to a SCIF using physical, electronic, or human controls.

Access Roster: A database or list of individuals, by name, who are currently authorized access to a particular level of SCI.

Access Suspension: The temporary withdrawal of one's access to SCI due to a circumstance or incident that has a bearing on SCI eligibility.

Access: The term used to denote the authorization which permits an individual to be exposed to classified information.

Accountable SCI: SCI determined by the SCI Executive Agent to be of critical enough sensitivity as to require the most stringent protection methods.

Accreditation:

- The formal certification by Physical Security Unit (PSU), Security Division, that a facility meets DCID 6/9 physical and technical security requirements;
- The official management decision to permit operation of an information system in a specified environment at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards;

Activation: As used in this manual, when a COOP Plan has been activated, whether in whole or in part.

Adjudicate or Adjudication: The process of determining one's eligibility for access to classified information.

Adversary: An individual, group, organization or government that has the capability and intention of harming FBI operations or assets.

Alternate Facility: A location used to carry out essential functions in a COOP situation.
Application Programming: The development and maintenance of programs that form specific applications, such as payroll, inventory control, accounting, and mission support systems.

Authenticate: To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an Information System, or to establish the validity of a transmission.

Authentication: Security measure designed to establish the validity of a principal (transmission, message, or originator, device, service, process, or person) or a means of verifying an individual’s authorization to receive specific categories of information.

Authorized User: A user who has been granted permission to access a specified system or equipment.

Availability: As the term relates to information systems, timely, reliable access to data and information services for authorized users.

Biometrics: Automated methods authenticating or verifying an individual based upon their physical or behavioral characteristics.

Camouflage: The use of natural or artificial materials on personnel, objects, or positions (e.g., tactical) in order to confuse, mislead or evade the enemy or adversary.

Cellular Telephone: A short-wave analog or digital telecommunication device through which a subscriber has a wireless connection from a mobile telephone to a nearby transmitter.

Certification and Accreditation (C&A): A comprehensive process to ensure implementation of security measures that effectively counter relevant threats and vulnerabilities. C&A consists of several iterative, interdependent processes and steps whose scope and specific activities vary with the information system being certified and accredited.

Certification: Comprehensive evaluation of the technical and nontechnical security features of a system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Certified Couriers: Individuals whose primary responsibility is to courier classified material worldwide.

Certified TEMPEST Technical Authority (CTTA): An experienced and technically qualified U.S. Government employee who has met established certification requirements according to NSTISSC-approved criteria and has been appointed by a U.S. Government department or agency to fulfill CTTA responsibilities.

Channel: An information transfer path within a system. Channel may also refer to the mechanism by which the path is affected.
Classified Contract: Any contract that will or may require access to classified information.

Classified Information: Information that has been determined (pursuant to EO 12958, as amended or any predecessor order) to require protection against unauthorized disclosure and is marked to indicate its classified status when in digital or hard copy form. The levels Top Secret, Secret, and Confidential are used to mark and designate such information.

Clearing: Removal of data from an information storage device, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (e.g., keyboard strokes); however, the data may be reconstructed using laboratory methods. Cleared media may be reused at the same classification level or at a higher level. Overwriting is one method of clearing.

Close and Continuing Relationship: A relationship between two individuals, or group of individuals, characterized by frequent, deliberate, mutual contact and continuing for a period of time, suggesting the relationship is more than a casual acquaintance.

Closed Storage Secure Area: An approved space in which all classified and sensitive information (to include, paper, hard drives, crypto keys, etc) must be secured in a GSA-approved security container when the material is not in use and the space is not occupied.

Codeword: Any of a series of designated words or terms used with a security classification to indicate that the material classified was derived through a sensitive source of method, constitutes a particular type of SCI, and is therefore accorded limited distribution.

Cognizance: Refers to security control, responsibility, and jurisdiction of supported units.

Cognizant Security Authority (CSA): The single principal designated by a SOIC to serve as the responsible official for all aspects of security program management with respect to the protection of intelligence sources and methods, under SOIC responsibility.

Cohabitant: A person living in a spouse-like relationship with the individual requiring SCI access to classified information, but not necessarily dependent upon sexual relations.

Collaborative Computing: The applications and technology (e.g., white boarding, group conferencing) that allow two or more individuals to share information in an inter- or intra-enterprise environment enabling them to work together toward a common goal.

Collateral: Information identified as National Security Information under the provisions of EO 12958, but that is not subject to enhanced security protection required for SAP information.
**Command Center Team:** The team which directs emergency operations. In large facilities, the team should include the Designated Official; an Occupant Emergency Coordinator, a Floor Team Coordinator, a Damage Control Team Coordinator, a Medical Coordinator, an Administrative Officer, a Building Manager and a Physical Security Specialist.

**Command Center:** The location from which emergency operations are directed.

**Communications Security (COMSEC):** Protective measures to prevent unauthorized persons from receiving classified information via telecommunications.

**Compartmentation:** Formal systems of restricted access to intelligence activities. Such systems are established to protect the sensitive aspects of specific sources, methods, and analytical procedures of foreign intelligence programs.

**Compartmented Address Book (CAB):** A book listing the message addresses and DCS addressees of all organizations authorized to receive SCI materials.

**Compelling Need:** A signed determination by a SOIC or designee that services of an individual are deemed essential to operation or mission accomplishment.

**Compilation:** Term used when referring to certain separate pieces of information which are unclassified by themselves, but become classified when combined.

**Compromise:** The known or suspected exposure of classified information or material to an unauthorized person. The compromise of SCI is the loss of control over any SCI resulting in a reasonable assumption that it could have, or confirmation of the fact that it has become known to unauthorized persons.

**Compromising Emanations:** Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information systems equipment.

**Computer Operations:** The function responsible for performing the various tasks to operate the computer and peripheral equipment, including providing the tape, disk, or paper resources as requested by the application systems.

**Computer:** A programmable machine having the two principle characteristics of: (1) responding to a specific set of instruction in a well-defined manner and (2) executing a prerecorded list of instructions (software program). For the purpose of this manual, any electronic device controlling the monitor and accepting signals from the keyboard and pointing device, if any.

**Computer or Communications System (Information System):** Any telecommunications and/or computer system related equipment or interconnected system or subsystem of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, storage, or reception of voice and/or data, including software, firmware, and hardware.
Computerized Telephone System: A generic term used to describe any telephone system that uses centralized stored program computer technology to provide switched telephone networking features and services. CTSs are referred to commercially by such terms as computerized private branch exchange (CPBX), private branch exchange (PBX), private automatic branch exchange (PABX), electronic private automatic branch exchange (EPABX), computerized branch exchange (CBX), computerized key telephone systems (CKTS), hybrid key systems, business communications systems, and office communications systems.

Connection Plane: Two adjacent ports on a KVM switch restricted to connections of the same security classification. Ports A and B comprise Connection Plane 1; Ports C and D comprise Connection Plane 2.

Consultant: An individual who is not a U.S. Government employee who provides a service to an agency or department of the U.S. Government.

Contact: Any form of meeting, association, or communication in person, by radio, telephone, letter or other means, regardless of who initiated the contact or whether it was for social or official reasons. A contact has occurred even if no official business was discussed or requested.

Contractor Owned: Device, equipment, or item purchase by a contractor or vendor in support of an FBI contract.

Continuity of Government: Coordinated efforts to ensure that minimum essential functions are fulfilled during catastrophic emergencies, and to ensure the maintenance of enduring constitutional government.

Continuity of Operations: Activities engaged in to ensure that essential functions are performed.

Continuous Operations: An accredited facility where classified information may be handled, processed, discussed, stored, or destroyed whenever the facility is manned 24 hours every day.

Contracting Officer's Technical Representative (COTR) (Contract Monitor): Appropriately indoctrinated personnel (military or civilian) appointed by the Contracting Officer to monitor the day-to-day activities of classified contracts or serve as a technical representative.

Contractor or Contract Personnel: Individuals employed by a civilian company or corporate entity involved in a Government contractual effort to the FBI.

Contractor-Owned: Device, equipment or item purchased in support of an FBI contract.

Contractor, Licensee or Grantee: A current, prospective or former contractor, licensee or grantee of a U.S. agency or department.

COOP Event: Any event which causes the relocation of essential operations to alternate sites.

Countermeasure: Anything which effectively mitigates the risk so that the risk is reduced to an acceptable level.
Courier: A currently cleared person authorized in writing to hand carry classified information or material.

Critical Assets: Information Technology hardware, software, telecommunications and audiovisual equipment.

Critical Information: Specific facts about friendly (e.g., US) intentions, capabilities, or activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences or accomplishment of friendly objectives.

Damage: A loss of friendly effectiveness due to adversarial action. Synonymous with harm.

Data Administration: The function that plans for and administers the data used throughout the organization. This function is concerned with identifying, cataloging, controlling, and coordinating the information needs of the organization. Database administration is a narrower function concerned with the technical aspects of installing, maintaining, and using an organization's databases and database management systems.

Data Security: The function responsible for the development and administration of the information security program. This includes development of security policies, procedures, and guidelines and the establishment and maintenance of a security awareness and education program for employees. The data security function is also concerned with the adequacy of access controls and service continuity procedures.

Data: A representation of facts, concepts, information, or instructions suitable for communications, interpretation, or processing by humans or by a system. Any information, regardless of its physical form or characteristics, including written or printed matter; information systems (IS) storage media; maps, charts, paintings, drawings, films, photos, engravings, sketches, working notes, and papers; reproductions of such things by any means or process; and sound, voice, magnetic, or electronic recordings in any form.

Data Storage Media: Any electronic storage medium that can be inserted into and removed from a computing device. Examples are magnetic tapes, hard/fixed disks (internal and external), thumb drives, zip drives, floppy disks, various types of random access and read-only memory, flash memory, Compact Disks (CDs) and Digital Video Disks (DVDs).

Date-Time-Group (DTG): An electronic message identifier entered by the proper releasing authority (e.g., 261445Z MAR 04).

DD Form 254 (DoD Contract Security Classification Specification): Document that provides guidance to both the contractor and the government. It is a legal document that directs the contractor about the proper protection of classified material released under the contract.

Debriefing: The process of informing a person their need-to-know for access is terminated.

Declassification: The determination that classified information no longer requires, in the interests of national security, any degree of protection against unauthorized disclosure.
coupled with a removal or cancellation of the classification designation. When media is lowered to unclassified, it must be properly sanitized before it can be downgraded.

**Decompartmentation:** The removal of information from a compartmented system without altering the information to conceal sources, methods, or analytical procedures.

**Defense Clearance and Investigations Index (DCII):** A computerized central index of clearance and investigative information.

**Defense Courier Service (DCS):** A system that provides for the secure and expeditious transportation and delivery of qualified material which requires controlled handling by courier. DCS is the primary means of transferring SCI documents.

**Defense Industrial Security Clearance Office (DISCO) or Directorate for Industrial Security Clearance Review (DISCR):** Processes all DoD contractor security clearances.

**Defense Special Security Communications System (DSSCS):** Worldwide, special purpose communications system for processing formatted SIGINT and CRITIC messages, and other sensitive or privacy information.

**Defensive Security Briefing (DSB):** Formal advisories that alert traveling personnel to the potential for harassment, exploitation, provocation, capture, entrapment, or criminal activity.

**Degauss:** To neutralize or overcome the magnetic field of magnetic recording media to erase readable data. The degaussing process may be used to “clear” or “declassify” certain magnetic storage media.

**Degaussing:** A procedure that reduces the magnetic flux on data storage media to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process. It is also called demagnetizing.

**Derivative Classification:** The incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that applies to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

**Derogatory Information:** Information which indicates that permitting access to SCI may not be clearly consistent with the interests of national security. Derogatory information includes arrests, disciplinary actions, letters of counseling, letters of reprimand, driving under influence (DUI), and driving while intoxicated (DWI).

**Designated Accrediting Authority (DAA):** Official with the authority to formally assume the responsibility for operating a system at an acceptable level of risk.

**Designated Couriers:** Individuals whose temporary responsibility is to courier classified material.

**Designated Official:** The highest ranking official in a facility or his/her delegate.
Destruction of Media: The process of physically damaging media so that it is not usable as media, and so that no known method can retrieve data from it. Data storage media will be destroyed in accordance with approval FBI policy and methods.

Device: A unit of hardware, outside or inside the case of housing for the essential computer that is capable of providing input to the essential computer or of receiving output or both. The term peripheral is sometimes used as a synonym for device or any input/output unit.

Director of Central Intelligence (DCI): The title of the former head of the Intelligence Community. The title and function are superseded by the Director of National Intelligence.

Director of Central Intelligence Directive (DCID): A directive issued by the Director of Central Intelligence (new title is Director of National Intelligence (DNI)) which outlines general policies and procedures to be followed by intelligence agencies and organizations which are under his direction or overview. The DNI has statutory responsibility for the protection of intelligence sources and methods.

Director of National Intelligence: The President's principal foreign intelligence adviser appointed by him with the consent of the Senate to be the head of the Intelligence Community to discharge those authorities and responsibilities as they are prescribed by law and by Presidential and National Security Council directives.

Disclosure: Conveying classified or sensitive information to another person. See "Release."

Documents and Materials: Any recorded information, regardless of its physical form or characteristics, including, without limitation, written or printed matter, automated data-processing storage media; maps; charts; paintings; drawings; films photographs; engravings; sketches; working notes and papers; reproductions of such things by any means or process; and sound, voice, magnetic or electronic recordings in any form.

Downgrading: Changing a security classification from a higher to a lower level.

DSS (DoD's Defense Security Service): The Executive Agent for the NISP. DSS inspects and monitors contractors who require or will require access to, or who store or will store classified information. It further determines the eligibility for access to classified information by contractors and their respective employees.

Due Process: Advising an individual that he or she has been determined ineligible for SCI access. This process gives reasons for the denial and affords the person an opportunity to appeal the decision.

Electronic Processing: The capture, storage, manipulation, reproduction, or transmission of data in all forms by any electronically-powered device. This definition includes, but is not limited to, computers and their peripheral equipment, word processors, office
equipment, telecommunications equipment, facsimiles, and electronic accounting machines, etc.

**Eligibility:** The determination by competent authority that a person is eligible for access to classified information.

**Emergency Action Plan (EAP):** Plan to be used during natural disasters, hostilities, or other emergencies.

**Encryption:** A method of applying a cryptographic key to plain text to encipher or encrypt thereby protecting the data from those not in possession of the key.

**End-user Computer:** A computer, the primary purpose of which is to accept input from and provide output to one human being at a time. It is contrasted with a "server" which serves many people. Examples of end-user computers are workstations, desktops, and laptops.

**Erasure:** Process intended to render magnetically stored information irretrievable by normal means.

**Essential Functions:** Functions that make it possible to provide vital services, exercise civil authority, maintain the safety and well being of the general populace, and sustain industrial and economic bases during emergencies.

**Essential Resources:** Resources that support the ability to provide vital services, exercise civil authority, maintain the safety and well being of the general populace, and sustain industrial and economic bases during emergencies.

**Executive Agent Program:** A program wherein a single department, agency, or organization collects or processes foreign intelligence at the direction of the Director of Central Intelligence (DCI) or higher national authority.

**Executive Order (EO):** A rule or order signed by the President.

**Expired Password:** A password that is no longer valid for a given User ID.

**Exploitation:** The process of obtaining intelligence information from any source and taking advantage of it.

**Facility Clearance:** An administrative determination that a contractor facility is eligible, from a security viewpoint, for access to NSI of the same or lower classification level as the clearance being granted.

**FBI Information:** Information, in any format, which is created, acquired or used in support of FBI business, is considered either owned by the Director FBI or in FBI custody and is known as FBI information.

**FBI-Controlled Facility:** Any room, group of rooms, building, or installation for which the FBI has administrative, management, or security control.

**Finished Intelligence:** The result of the production step of the intelligence cycle—the intelligence product. Intelligence information that has been analyzed, compared with information from other sources and made into a product.
Firewall. System designed to defend against unauthorized access to or from a private network.

Firmware: A combination of software and hardware. ROMs, programmable read-only software (programs or data) that has been written on read-only memory.

Fixed Input/Output (I/O) Device: A storage device not designed for easy portability such as a fixed hard drive.

Foreign Integrated Person (FIP): A foreign national who is assigned to the FBI in accordance with the terms of an exchange agreement and who performs duties prescribed by a position description according to an approved security plan.

Foreign Liaison Official: Foreign officials, usually locally based, involved in liaison activities with FBI officials on a regular and frequent basis.

Foreign National: Any individual who is not a citizen of the U.S. by birth or through naturalization, including resident aliens, students, refugees, and émigrés. The term “foreign national” and “non-U.S. Citizen” may be used interchangeably.

Formal Access Approval: Documented approval to allow access to a particular category, or classification level, of information.

General User: An individual who uses a computer. This ranges from expert programmers to novices and includes any individual who run an application program. General users are only given limited access privileges to their personal computer and that information for which they have the appropriate clearance and established need-to-know.

Government-Owned: Device, equipment or item purchased by the government, directly or through a third-party contract.

Hardcopy Document: Any document that is initially published and distributed by the originating component in physical form and that is not stored or transmitted by electrical means.

Hash Total: Value computed on data to detect error or manipulation.

Hookswitch: The device used to determine whether or not the handset is in place in or on the handset mounting. In some cases the hookswitch will not involve any sort of mechanical switch and/or break any incoming current loop.

Hosted Visit: A visit by official personnel of a foreign government under the auspices of an invitation that is approved by an FBI Division Head.

Identification: The means by which a user provides a claimed identity to the Information System. Process an IS uses to recognize an entity (cnissi 4009).
Image Recording Devices: Handled devices that are capable of recording moving or still images and sound including cellular telephones with integrated recording components, single lens reflex cameras, specialty cameras, web cams, disposable and novelty cameras.

Immediate Family Member: The spouse, parents, brothers, sister, and children. Immediate family members also include step and foster parents; half, step, and foster siblings; and adopted step and foster children, provided that a close relationship existed or exists as evidenced by substantial period of common residence. Cohabitant, with whom an intimate relationship is maintained, is also considered to be immediate family members of the individual requiring SCI access, per DCID 6/4.

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 each individual who has been approved for access prior to his exposure.

Information: The intelligence derived from data on or about a system, or the intelligence obtained from the structure or organization of that data.

Information Availability: Assuring that information is accessible to authorized users when needed and, to the extent possible, that information systems are safe from accidental or intentional disablement.

Information Confidentiality: Assuring that information is accessible only as authorized and that it cannot be acquired by unauthorized personnel and/or by unauthorized means.

Information Integrity: Assuring that information is kept in tact, and not lost, damaged, or modified in an unauthorized manner.

Information System: Any telecommunication and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data (digital or analog: includes software, firmware, and hardware.

Information System Security Manager (ISSM): The individual assigned responsibility for managing the security posture of an FBI information systems site.

Information System Storage Media and Equipment: The physical storage devices used by an IS upon which data is recorded including storage media internal to IS equipment such as printers, copiers, and faxes. IS storage media may be grouped according to similarities and common-properties in regard to technology, applications, or processing requirements as: Flexible Magnetic Storage (magnetic cards, floppy disks, diskettes, magnetic tape-on reels and in cassettes, Rigid Magnetic Storage (removable disk packs-single and multiple platter disk packs, unsealed disk packs, hard disk assemblies, magnetic Bernoulli cartridges); Magnetic Memory Devices (bubble memory units, core memory); Optical Storage (optical disks, optical tape, compact disks, optical
Bernoulli cartridges); and Semiconductor Memory Devices (RAM, ROM, PROM, EPROM, etc.)

**Information Technology Security Incident:** A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security policies. These IT security incidents normally fall into the following categories (1) attempts (either failed or successful) to gain unauthorized access to a system or its data, (2) unwanted disruption of denial of service, (3) the unauthorized use of a system for the processing or storage of data, (4) changes to systems hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent or (5) spillage or contamination of the system by the introduction of information classified at a higher level that the system is authorized to process.

**Input/Output Device:** A unit of hardware, outside or inside the case or housing for the essential computer that is capable of providing input to essential computer or receiving output or both. The term peripheral is sometimes used as a synonym for device or any input/output (I/O) unit.

**Intelligence Community (and agencies within the Intelligence Community):** A collective term referring to the agencies or organizations and activities which conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States.

**Intelligence Cycle:** Process by which information is acquired and converted into intelligence and made available to the customers.

**Intelligence Information:** Foreign intelligence and foreign counterintelligence, whose sources or methods of acquisition are considered sensitive. This information is classified pursuant to Executive Order 12958, as amended. Intelligence information includes, but is not limited to, SCI.

**Intelligence Sources and Methods:** Comprised of the classified sources and methods the DCI protects under Section 102 of the National Security Act of 1947 and Executive Order 12333.

**Interface:** The connection and interaction between hardware, software, and the user.

**Interim Security Clearance:** A security clearance based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

**Interoperability:** The ability of communications systems to directly and satisfactorily exchange information among users.

**Interoperable Communications:** Alternate communications which provide the ability to perform essential functions, in conjunction with other agencies, until normal operations can be resumed.

**Intrusion Detection:** The process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusion.
Intrusion Detection System: A software or hardware device that automates the intrusion detection process. Intrusion Detection Systems are made up of three functional components: Information sources, analysis, and response. The system obtains event information from one or more information sources, performs a pre-configured analysis of the event data and generates specified responses, ranging from reports to active intervention when intrusions are detected. Intrusion Detection Systems serve as real-time monitoring mechanisms, watching activities and making decisions about whether the observed events are suspicious.

Investigation: A duly authorized, systematic, detailed examination or inquiry to develop the facts and determine the truth of a matter. If predicated by an adverse allegation, the investigation will attempt to prove or disprove the allegation in question.

Keyboard: A device that converts the physical action of a user, such as the depressing of keys, into electronic signals corresponding to a character in the form of an electronic alphabet.

Key Management Personnel: Owners, officers, directors and executive personnel of a vendor.

Laptop Computer/Tablet PC: A battery or AC powered computer generally smaller than a briefcase that can easily be transported and conveniently used in temporary spaces.

Law Enforcement Sensitive (LES): Unclassified information is originated by the FBI that may be used in criminal prosecution and requires protections against unauthorized disclosure to protect sources and methods, investigative activity, evidence, and the integrity of pretrial investigative reports.

Least Privilege: Identifying a user’s job functions, determining the minimum set of privileges required to perform that functions, and restricting the user to a domain with those privileges and nothing more.

Level-of-Concern: A rating assigned to an information system by the DAA. A separate Level-of-Concern is assigned to each IS for confidentiality, integrity, and availability. The Level-of-Concern for confidentiality, integrity, and availability can be Basic, Medium, or High. The Level-of-Concern assigned to an IS for confidentiality is based on the sensitivity of the information it maintains, processes, and transmits. The Level-of-Concern assigned to an IS for integrity is based on the degree of resistance to unauthorized modifications. The Level-of-Concern assigned to an IS for availability is based on the needed availability of the information maintained, processed and transmitted by the system for mission accomplishment, and how much tolerance for delay is allowed.

Library Management/Change Management: The function responsible for control over program and data files that are either kept on line or on tapes and disks that are loaded onto the computer as needed. This function also is often responsible for controlling documentation related to system software, application programs, and computer operations.

Limited Access Authorization (LAA): Authorization for access to CONFIDENTIAL or SECRET information granted to non-US citizens and immigrant aliens, which is limited
to only that information necessary to the successful completion of their assigned duties and based on a background investigation scoped for 10 years.

**Limited Dissemination (LIMDIS):** A telecommunications caveat that may be used with a classified message to limit distribution within the addressed activity. However, the limited distribution caveat does not effectively restrict processing, handling, and distribution of electrically transmitted messages within electronic message processing systems.

**Logical Access Controls:** The system-based mechanisms used to specify who or what (e.g., in the case of a process) is to have access to a specific system resource and the type of access that is permitted.

**Magnetic Media:** Media with a surface layer containing particles of metal or metallic oxide that can be magnetized in different directions to represent bits of data, sound, or other information. Floppy disks, tape cartridges, writable CDs, and hard drives.

**Magnetic Remanence:** Magnetic representation of residual information remaining on a magnetic medium after the medium has been cleared. See clearing.

**Malicious Code:** Software designed specifically to damage or disrupts a system, such as a virus or a Trojan horse. There are more than 50,000 known malicious code entities that have made the rounds of the Internet.

**Malicious Software (Malware):** Software programs designed to compromise or interrupt computer systems, networks or data.

**Manual of Administrative Operations and Procedures (MAOP):** The FBI manual containing rules and regulations of a personnel nature and information which pertains to the administrative operations of a field office and some instructions for FBI Headquarters.

**Manual of Investigative Operations and Guidelines (MIOG):** The FBI manual describing the FBI’s investigative authority, responsibilities, and guidelines.

**Markings:** Markings on documents or other classified media that indicate a variety of information such as classification, the identity of the original classification authority, declassification instructions, a reason for classification, specific security control system for the document (if required), and in particular, dissemination controls. This term covers all handling caveats that restrict dissemination of classified intelligence.

**Memorandum of Agreement (MOA):** Written agreement with a CSA allowing another CSA joint use of a contractor SCIF.
Microfiche: A sheet of microfilm containing multiple micro-images in a grid pattern, or array of micro-images on a transparent sheet.

Microfilm: A film bearing a photographic record of printed or other graphic matter on a reduced scale.

Minor Derogatory Information: Information that, by itself, is not of sufficient importance or magnitude to justify an unfavorable administrative action in a personnel security determination.

Mission Critical Data: Information essential to supporting the execution of essential functions.


Monitor: A computer output surface and projecting mechanism that shows text and other graphic images from a computer system to a user, using a Cathode Ray Tube (CRT), Liquid Crystal Display (LCD), Light-Emitting Diode (LED), gas plasma, active matrix or other image projection technology. The display (the terms display and monitor are often used interchangeable) is usually considered to include the screen or projection surface and the device that produces the information on the screen. In some computers, the display is packaged in a separate unit called monitor. Displays (and monitors) are also sometimes called Video Display Terminals (VDTs). Also included in this category are tactile Braille output devices.

Multiple-level Operating Environments (MLOE): Infrastructure and client services that allow access to computing resources at different classification or sensitivity levels from a single client system.

National Disclosure Policy (NDP): National policies and procedures governing foreign release of US classified military information to foreign governments and international organizations. The NDP is based on NSDM 119, July 1971.

National Foreign Intelligence Board (NFIB): An organization composed of representatives from intelligence organizations of the US Government, established in accordance with the National Security Act of 1947 to oversee security and intelligence matters of the United States. The Board is chaired by the Director of Central Intelligence (DCI).

National Interest Determination: Justification for a company cleared under a Special Security Agreement through the Department of Defense (DoD), National Industrial Security Program (NISP), to provide special authorization for the contractor's access to proscribed information.

National Security Information (NSI): Includes any information that has been determined pursuant to EO 12958, as amended, or any predecessor order to require protection against unauthorized disclosure and that is so designated. The levels Top Secret, Secret, and Confidential are used to designate such information.

National Security: The national defense and foreign relations of the U.S.

Need-to-Know: A determination by an authorized holder of classified information that access to specific classified material in their possession is required by another person to perform a specific and authorized function to carry out a national task.

Network Administration: The function responsible for maintaining a secure and reliable online communications network and serves as liaison with user department to resolve network needs and problems.

Non-Accountable SCI: SCI material that does not require document accountability.

Nondisclosure Agreement (NdA): A written, legally binding agreement (FD Form 4414 or SF-312) signed by a candidate for access to classified information. The candidate promises not to disclose SCI to unauthorized individuals. NdA is the preferred acronym.

Non-Operational Spaces: Any FBI facility, room, area where classified and sensitive information is prohibited from being processed, discussed, and stored (e.g., lobby).

Non-Volatile Memory: Memory components that can be erased or reused. Erasable Programmable Read-Only Memory (EPROM) and Electronically Erasable Programmable Read Only Memory (EEPROM) are types of non-volatile memory.

Novelty Image Cameras: Image recording devices that are incorporated into objects such as toys and watches.

OADR: An obsolete declassification marking meaning “Originating Agency’s Determination Required.” The originator has to approve any declassification action.

Occupant Emergency Organization: Generally consists of a Command Center Team, Floor Teams and a Damage Control Team. Organization members should be provided with visual identifiers such as colored hats or arm bands.

Occupant Emergency Plan: A detailed security program guidance document denoting the organization and emergency response procedures that are required for the evacuation of a facility under emergency conditions.

Occupant Emergency Program: A short-term emergency response program, establishing procedures for safeguarding lives and property during emergencies in particular facilities.

Oersted: The unit of measure of the magnetic field.

Off-Sites: Any FBI leased space that is not a Field Office or Resident Agency (e.g., lookouts, ETI/Technical facilities, automotive units, etc.).

Off-Hook (Telephone): A telephone that is in the in-use state.

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

On-Hook (Telephone): A telephone that is in the idle state.
On-Hook Telephone Audio Security: The use of positive measures to protect on-hook telephones against passing room audio is known as on-hook audio security or on-hook telephone audio security.

Open Source Intelligence (OSINT): Information of potential intelligence value that is available to the general public.

Open Storage Secure Area: An approved space for the open storage of material up to and including the Secret collateral level.

Optical Media: Storage medium from which data is read and to which it is written by lasers. Optical media offers no mechanism for sanitization and must be destroyed by NSA-approved methods.

Orders of Succession: Provisions for the assumption of senior offices in the event that during emergencies officials unavailable to execute their duties.

Original Classification: An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

Overwriting Media: A software procedure that replaces the data previously stored on magnetic storage media with a predefined set of meaningless data. Overwriting is an acceptable method for clearing media. Overwrite all data storage locations three times; the first time with a random character, the second time with a specified character, and the third time with the complement of that specified character.

Password: A private alpha-numeric character string used to authenticate an identity. Knowledge of the password that is associated with a User ID is considered one form of proof of identity. Protected/private string of letters, numbers and special characters used to authenticate an identity or to authorize access to data.

Password Authentication Process: The actions involving (1) obtaining an identifier and a personal password with the stored, valid password that was issued to or selected by the person associated with that identifier; and (3) permitting access to the Information System if the entered password and the stored password are the same.

Password Lifetime: It is the maximum acceptable period of time that a password is valid and can be used.

Password System: A system that uses a password to authenticate an entity’s identity or to authorize an entity’s access to data and which consists of means for performing one or more of the following password operations: generation, distribution, entry, storage, authentication, replacement, or cryptographic operations performed on passwords.

Patch (also called a service patch): It is a fix to a program bug. A patch is an actual piece of object code that is inserted into (patched into) an executable program. Patches typically are available as downloads over the Internet.

PBX (Private Branch Exchange): A PBX is a local switched telephone network that is itself a member of the PSTN, and provides access to the PSTN for its member terminals.
Periodic Reinvestigation (PR): An investigation conducted at a specified interval for the purpose of updating a previously completed background investigation, special background investigation, or single scope background investigation, or PR.

Permanent Certification or Perm-cert: A perm-cert certifies a person's access to another organization for a specific period, not to exceed 3 years.

Personal Digital Assistant (PDA): A mobile hand-held device that provides computing and information storage and retrieval capabilities.

Personal Digital Assistant (PDA): A generic term for a class of small, easily carried electronic devices used to store and process information. PDAs do not include wireless technology.

Personally Owned: Device, equipment or item purchased with other than Government or contractor funds. An item that is not government owned or managed.

Personnel Security Investigation (PSI): Any investigation required for the purpose of determining the eligibility of personnel, contractor employees, consultants, and other persons affiliated with the FBI, for access to classified information, assignment or retention in sensitive duties, or other designated duties requiring such investigation.

Plain Language Address (PLA): A phrase used to denote the abbreviated language coding of an activity short title used in message addressing.

Portable Electronic Device (PED): Any non-stationary electronic device with the capability of processing, storing, and/or transmitting information. This definition includes, but is not limited to, PDAs, cellular phones, two-way pagers, e-mail devices, audio/video recording devices, hand-held/laptop computers.

Possible SCI Compromise: A security violation or incident in which immediately available circumstances do not rule out SCI compromise.

Pouching: The proper packaging of SCI documents for transmission by DCS or authorized couriers.

Practice Dangerous to Security (PDS): A failure to comply with the provisions of security regulations or this manual causing a potential compromise of classified information.

Primary Facility: The site of normal operations.

Prime Tenant: An organization with the largest number of employees in a facility.

Principal Accrediting Authority (PAA): The agency head having the authority and responsibility for all information systems (except intelligence systems) within an agency. The Director, Central Intelligence (DCI) is the PAA for all intelligence systems.

 Principle of Least Privilege: The principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of a computer.
Privacy Communications Channel: A system known as “back channel” or “black book” support. It is authorized by the Secretary of Defense for senior defense officials to exchange messages that discuss highly sensitive or privileged matters. These messages require greater limited distribution and restricted handling than normally provided by ordinary communications means.

Privilege User: An individual who has access to system control, monitoring, or administration functions (e.g., system administrator, system ISSO, maintainers, system programmers, etc.). A user who, by virtue of function, and/or seniority, has been allocated.

Product: An intelligence report disseminated to customers. In SIGINT use, it is intelligence information derived from the analysis of SIGINT materials, which is published as a report or translation for dissemination to customers.

Production Control and Scheduling: The function responsible for monitoring the information into, through, and as it leaves the computer operations area and for determining the succession of programs to be run on the computer.

Protected Distribution System (PDS): A communications system to which electromagnetic and physical safeguards have been applied to permit secure electrical transmission of unencrypted classified SCI which has been approved by the cognizant SOIC.

Protection Level: An indication of the implicit level of trust that is placed in a system’s technical capabilities. A protection level is based on the classification and sensitivity of information processed on the system relative to the clearance(s), formal access approval(s), and need-to-know of all direct and indirect users that receive information from the IS without manual intervention and reliable human review.

Proximity Access/Approval: An approval to persons who closely support SCI collection, processing, or use, but whose duties do not warrant granting substantive SCI access approvals. It may be granted by, and at the discretion of, the cognizant SOIC.

Purging: Rendering stored information unrecoverable. See Sanitize.

Quality Assurance/Testing: The function that review and tests newly developed systems and modifications to determine whether they function as specified by the user and perform in accordance with functional specifications. Testing may also determine whether appropriate procedures, controls, and documentation have been developed and implemented before approval is granted to place the system into operation.

Raw Intelligence: Collected intelligence information that has not yet been converted into finished intelligence.
Real Property: Overt and covert facilities either federally owned or privately owned and leased through GSA or by the FBI to include, but not limited to, buildings, office suites, office spaces, houses, apartments, laboratories, garages, warehouses, and hangers.

Recipient: A person authorized to receive or have knowledge of SCI activities.

Reconstitution: The process by which surviving and/or replacement personnel resume normal operations at the original primary or a replacement site.

Release of Information: The release of SCI to an authorized recipient, to include oral, visual, or actual physical release of the information.

Release: The physical transfer of tangible products to an authorized recipient for retention. Thereafter the recipient assumes responsibility for the physical security of and all personnel access to the products in accordance with classification and/or special handling control specified for the product.

Remanence: Residual information remaining on storage media after clearing. See magnetic remanence and clearing.

Removable IS Storage Media: Includes magnetic tape reels, disk packs, diskettes, CD-ROMs, removable hard disks, disk cartridges, optical disks, paper tape, reels, magnetic cards, tape cassettes and micro-cassettes, and any other devices on which data is stored and which normally is removable from the system by the user or operator.

Removable Thumb Drive: A non-volatile device similar to EEPROM where erasing can be done in blocks or the entire chip. This is known as flash thumb drives, pen drives, flash memory, and flash memory sticks.

Reproduction Equipment: A class of equipment such as copiers, facsimile machines, and scanners that may be used to reproduce documents. This equipment may be connected to a network, contain a modem for remote access, or exist in a stand alone mode.

Residual Data: Any data that remains stored on one of the reproduction equipment data storage components even document reproduction taken place.

Residue: Data left in storage after information processing operations are complete, but before degaussing or overwriting has taken place. Any physical state remaining on storage media after erasing or overwriting which correlated with previously stored information.

RF Capabilities: As used in this policy, any PED radio frequency transmitter, except single-function cell phones which are addressed separately.

Risk Analysis: An assessment of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence.
Risk Management: The total process of identifying, measuring, and minimizing uncertain events affecting system or network resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluations, safeguard implementation, and systems review.

Risk of Capture Briefings: Advisories that alert personnel as to what may be expected in the way of attempts to force or trick them to divulge classified information if captured or detained and that offer suggested courses of action they should follow to avoid or limit such divulgence. These advisories include instructions/advice for advance preparation of innocuous, alternate explanations of duties and background.

Risk: The expected loss from an attack or incident. For an attack/defense scenario, risk is assessed as a combination of threat (expressed as the probability that a given action, attach, or incident will occur, but may also be expressed as frequency of occurrence), vulnerability (expressed as the probability that the given action, attack, or incident will succeed, given that the action, attack, or incident occurs) and consequence (expressed as some measure of loss, such as dollar cost, resources cost, programmatic impact, etc.). The total risk of operating a system is assessed as a combination of the risks associated with all possible threat scenarios. Risk is reduced by countermeasures.

Sanitization:
- The process of editing or otherwise altering intelligence information or reports to protect/conceal sensitive intelligence sources, methods, capabilities, and analytical procedures to permit dissemination of information outside compartmented systems.
- A process of removing information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.

Sanitize: To remove or conceal from view of non-SCI indoctrinated persons granted entry to a SCIF on a legitimate temporary basis; for example, janitorial, maintenance, inspection or similar personnel.

SCI Access Determination Authority: The individual designated by a Senior Official of the Intelligence Community to make SCI access, denial, and revocation determinations.

SCIF Closed Storage: An accredited space in which classified materials must be secured in a GSA-approved security container.

SCIF Open Storage: An accredited space for the open storage of material up to and including TS-SCI.

SCI Security Official: Personnel appointed to be the focal point for the receipt, control, and accountability of SCI, provide advice and assistance, and have day-to-day SCI security cognizance over their offices and subordinate SCIFs in the local area. For purposes of this manual, SCI Security Officials normally refer to the SSO and the SSR.

SCIF Responsible Security Officer: The security officer with primary responsibility for the security of a SCIF.

Scope: The time period to be covered and the sources of information to be contacted during the prescribed course of a PSI.
Security Assurance: The written confirmation requested by and exchanged between governments, of the security clearance level or eligibility for clearance of their government representative. It includes a statement by a responsible official of a foreign government or international organization that the recipient of the US classified information possesses the requisite security clearance. It also indicates that the original recipient is approved by his or her government for access to information of the security classification involved and that the recipient government will comply with security requirements specified by the United States. The security assurance will include the visitor's full name, title/affiliation, date and place of birth.

Security Clearance: A determination that a person is eligible under the standards of Executive Order 12968, for access to classified information.

Security Critical Patch: A severity level of the patch or update as determined by issuing authority. This severity level of patch or update will have a mandatory compliance data published in the associated alert. Typically, critical patches correct vulnerabilities that are well known, widespread, allow an attacker to do significant damage (i.e., inability of the organization to accomplish its mission) and for which exploits have been developed and are easily employed.

Security Incident: A failure to safeguard FBI classified and sensitive material according to FBI policies and Director of Central Intelligence directives. Security incidents are segregated into security violations or security infractions.

Security Infraction: An incident that is not in the best interest of security which does not involve the loss, compromise, or suspected compromise of classified national security information (e.g., leaving a security container unlocked at the end of a workday).

Security Labeling: Information representing the sensitivity of a subject or object, such as its classification (Unclassified, Confidential, Secret, and Top Secret) together with any applicable handling caveats (e.g., ORCON, FOUO, LES, and SCI Caveats).

Security Low Patch: Low urgency patches correct vulnerabilities that are relatively unknown, would be extremely difficult to exploit and/or, if exploited, would have little if any impact on the ability of the organization to accomplish its mission.

Security Moderate Patch: Moderately urgent patches correct vulnerabilities that are well known but more difficult to exploit and for which no exploits are known to exist: Exploits that are known are difficult to employ successfully or may be defeated by defenses other than implementation of the patch, expose the enterprise to moderate damage (i.e.; severely impair the organization's ability to accomplish its mission).

Security Patch: A patch that corrects a vulnerability that jeopardizes the software's integrity or availability or that jeopardizes the integrity, availability or confidentiality of the data processed by the software.

Security Systems or Devices: A group of interacting or single mechanical or electrical elements that provide protection from unauthorized use or entry. Examples of security systems or devices include, but are not limited to, walk-through metal detectors, access...
control security turnstiles, intrusion detection equipment or systems, access control card reader systems, and vehicle barriers.

**Security Violation**: A compromise of classified information to persons not authorized to receive it or a serious failure to comply with the provisions of security regulations or this manual which is likely to result in compromise.

**Semi-Permanent SCIF**: Vehicles with mounted shelters or towed trailer type shelters that are accredited as SCIFs.

**Senior Officials of the Intelligence Community (SOIC)**: The heads of agencies and organizations identified in section 3.4(f) (1 through 6) of Executive Order 12333 or successor orders, directives, or laws.

**Sensitive But Unclassified (SBU) Information**: Information that requires protection due to the risk or magnitude of loss or harm that could result from inadvertent or deliberate disclosure, modification and/or destruction of the information. The term includes information, the improper use or disclosure of which could adversely affect the ability of the FBI to accomplish its mission; information that is investigatory in nature; grand jury information subject to the Federal Rules if Criminal Procedure, Rule 6(e), Grand Jury Secrecy of Proceedings and Disclosure; proprietary information; records about individuals requiring protection under the Privacy Act; information not releasable under the Freedom of Information Act; and information which could be manipulated for personal profit or to hide the unauthorized use of money, equipment, or privileges. Also referred to as Limited Official Use Information.

**Sensitive Compartmented Information (SCI) Access Eligibility**: A determination that a person is eligible for SCI under the personnel security standards of DCID 6/4.

**Sensitive Compartmented Information (SCI)**: Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

**Sensitive Compartmented Information Control Channels**: A method or means expressly authorized for the handling or transmission of SCI whereby the information is provided exclusively to indoctrinated persons.

**Sensitive Compartmented Information Facility or SCI Facility (SCIF)**: An accredited area, room, group of rooms, buildings, or installations where SCI may be stored, used, 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.

**Sensitive Information**: Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs or the privacy to which individuals are entitled under [The Privacy Act], but has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.
Service Cryptologic Element (SCE): Those elements of the US Army, Navy, and Air Force which perform cryptologic functions; Navy and Air Force elements are also known as Service Cryptologic Agency(ies).

Signals Intelligence (SIGINT): A category of intelligence comprising either individually or in combination all communications intelligence, and foreign instrumentation signals intelligence, however transmitted.

Significant Derogatory Information: Information that could, in itself, justifies an unfavorable administrative action, or prompts an adjudicator to seek additional investigation or clarification.

Significantly Modified: An information system is significantly modified when its data content, user population, connectivity, or its threat environment is extended beyond the bounds of its accreditation.

Single-Function Cellular Phone: A cell phone with no additional capabilities. It can only be used for voice communications over a cellular network, but may have the capability to provide text messaging. Storage of speed dial and Caller ID type information is permitted.

Single Scope Background Investigation (SSBI): An investigation completed according to DCID 6/4, meeting the investigative scope requirements for Top Secret and 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 within a ten-year scope. Final SCI adjudication will be held in abeyance pending completion of the investigation.

Special Access Program (SAP): Any program, which may or may not contain SCI, imposing need-to-know and access controls beyond those normally provided for access to Confidential, Secret, and Top Secret information. Such controls may include, but are not limited to, access approval; adjudicative or investigative requirements; special designation of officials authorized to determine need-to-know; or special list of persons determined to have a need-to-know.

Special Investigative Inquiry (SII): A supplemental personnel security investigation of limited scope, to prove or disapprove relevant allegations that have arisen concerning a person upon whom a personnel security determination has been previously made, and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a personnel security determination.
Special Purpose Access (SPA): An access granted to persons who require SCI access for short periods (not to exceed 90 days).

Special Security Officer (SSO): The SSO is responsible for the security management, operation, implementation, use and dissemination of all COMINT and other types of SCI material within his respective organization.

Special Security Representative (SSR): A person responsible, under the direction of the servicing/supporting SSO, for the day-to-day management and implementation of SCI security and administrative instructions for a separate subordinate SCIF.

Specialty Cameras: Electronic devices that have the capability to digitally record images and audio. These electronic devices consist of cellular telephones, web cams, and personal electronic devices.

Specific Liaison Visits: Foreign officials involved in liaison activities with the FBI whose visit is for a one-time meeting with FBI officials.

Spyware: A software component that collects information used to develop a profile of user activities or system performance; some spyware is dangerous in the same sense as malicious software, but also affects user privacy and intellectual property rights.

Standard Levels of Classification: The three classification designations of Top Secret, Secret, and Confidential established by Executive Order 12958.

Standard Operating Procedure (SOP): A written procedure that provides an index of major topics.

Strong Password: A password that is difficult to decipher by both humans and computer programs, effectively protecting data from unauthorized access. The security afforded by passwords is determined by the probability that a password can be guesses during its lifetime. All else being equal the longer the password and the larger the possible character set available for use, the greater the security the strong password provides. Given today's technology, a password can be considered sufficiently strong enough to successfully resist continuous guessing for its lifetime when it consists of at least eight characters that are a combination of letters (both upper and lower case), numbers and special characters (@, #, $, %, etc.).

Superuser: A privilege user who has unrestricted access to the whole information system.

Surreptitious Entry: Unauthorized entry in a manner which leaves no readily discernible evidence.

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.

Switch: A device permitting a single set of peripherals to be shared among two or more computers, synonymous with KVM switch in this Policy.
System: A network of structures and channels as for communications and information. A generic term used for briefness to mean either a major application or a general support system.

Tactical or Combat Operations: Operations that are conducted under combat or simulated combat conditions (to include ground, airborne, and shipboard), that provide for a mobile or non-permanent SCIF environment.

TEMPEST: An unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are unintentional intelligence-bearing signals that, if intercepted and analyzed, will disclose classified information when it is transmitted, received, handled, or otherwise processed by any information processing equipment.

Temporary Secure Working Area (TSWA): A temporarily accredited facility that is used no more than 40 hours monthly for the handling, discussion, or processing of SCI.

Terrorism: Premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine state agents, usually to influence an audience.

Tests, Training and Exercises: Measures to ensure that COOP Plans are capable of supporting the continue execution of essential functions.

Threat: Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

Trojan Horse: Computer program containing an apparent or actual useful function that contains additional (hidden) functions that allow unauthorized collection, falsification or destruction of data.

1SG-Approved Telephone: 1SG-approved status is awarded to telephones that have been technically evaluated by the government’s Telephone Security Group and determined to meet all applicable on-hook audio security criteria. A 1SG-approved telephone provides all necessary security features as intrinsic properties of the telephone itself.

Unclassified Information: Information that has not been determined under Executive Order 13292, or by any successor order, Executive Order 12951, or any successor order,
or the Atomic Energy Act of 1954 (42 USC 2011) to require protection against unauthorized disclosure.

**United States Citizen (Native Born):** A person born in one of the 50 United States, Puerto Rico, Guam, American Samoa, Northern Mariana Islands, US Virgin Islands, or Panama Canal Zone (if the father and/or mother was or is a US citizen).

**United States Visitor:** A visitor who is a citizen of the United States.

**Universal Serial Bus (USB):** A form of Electronically Erasable Programmable Memory (EEPROM), non-volatile storage media with special properties such as small size, mobility, connectivity, compatibility, and storage density. USB connections attach personal computers to keyboards, printers, thumb drives and other peripherals, delivering power to devices on the bus and eliminating separate power cords. The USB standard provides a data rate of 12 megabytes per second and supports up to 127 devices. It is slower than its rival FireWire (IEEE 1394) but is less expensive to implement. USB delivers complete plug-and-play capabilities to electronic devices as well as hot-swap capabilities. Because of the small size of the USB connector, it can be used on notebook and handheld computers.

**Unofficial Travel:** Travel undertaken by an individual without official, fiscal, or other obligations on the part of the U.S. Government (i.e. personal travel).

**Upgrading:** The determination that certain classified information requires, in the interests of national security, a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect the higher degree.

**User:** The human operator of the reproduction equipment.

**User Agency SSO:** The SSO directly supporting an SCI contract.

**User ID:** A unique character string that is used by an ADP system on a comparison basis to help establish the identity of the user. The security provided by a password system does not rely on the secrecy of the user's ID.

**Validate:** To confirm the validity of a request for a SCIF, communications equipment, circuit, ADP system, and/or special purpose access request.

**VIP (Very Important Person):** Visitor's equivalent to the position of an FBI Assistant Director or higher, heads of state, ambassadors, and similar titles or positions.

**Virus:** Independent program that replicates from machine across network connections often clogging networks and computer systems as it spreads.

**Vital Records:** Electronic and hard copy documents needed to support essential functions during a COOP situation.

**Voice Over Internet Protocol (VOIP):** A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network or across the Internet.
**Volatile Memory**: A digital electronic component found on circuit boards in copy machines that can be completely erased when the power is turned off for at least 30 seconds.

**Vulnerability**: A condition that is exploitable and that, when exploited, can directly lead to the death of FBI personnel, damage to FBI facilities, the loss or theft of NSI, the loss or theft of For Official Use Only information, or the compromise of FBI operations or activities. A weakness in system security procedures, administrative controls, internal controls, or others, which could be exploited to gain unauthorized access to classified or sensitive information.

**Vulnerability Assessment**: An evaluation, study or review to determine the vulnerability of a person, facility, information or operations to adversarial attack.

**Waiver**: Withdrawal or modification of certain requirements, usually mandatory for a position, facility, or action.

**Worm**: Independent program that replicates from machine to machine across network connections often clogging networks and computer systems as it spreads.
Appendix B: Keyword Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACF</td>
<td>Access Control Facility</td>
</tr>
<tr>
<td>AD</td>
<td>Assistant Director</td>
</tr>
<tr>
<td>AIS</td>
<td>Automated Information Systems</td>
</tr>
<tr>
<td>AMU</td>
<td>Assurance Management Unit</td>
</tr>
<tr>
<td>ATO</td>
<td>Authorization To Operate</td>
</tr>
<tr>
<td>ASU</td>
<td>Acquisition Security Unit</td>
</tr>
<tr>
<td>BMS</td>
<td>Balanced Magnetic Switch</td>
</tr>
<tr>
<td>C&amp;A</td>
<td>Certification and Accreditation</td>
</tr>
<tr>
<td>CAB</td>
<td>Cryptographic Access Briefing</td>
</tr>
<tr>
<td>CMAU</td>
<td>Critical Mission Assurance Unit</td>
</tr>
<tr>
<td>CARC</td>
<td>Community Acquisition Risk Center</td>
</tr>
<tr>
<td>CAPCO</td>
<td>Controlled Access Program Coordination Office</td>
</tr>
<tr>
<td>CBX</td>
<td>Computerized Branch Exchange</td>
</tr>
<tr>
<td>CCI</td>
<td>Controlled Cryptographic Item</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed Circuit Television</td>
</tr>
<tr>
<td>CCU</td>
<td>Contractor Clearance Unit</td>
</tr>
<tr>
<td>CD</td>
<td>Counterintelligence Division</td>
</tr>
<tr>
<td>CDF</td>
<td>Common Fill Device</td>
</tr>
<tr>
<td>CIK</td>
<td>Crypto Ignition Key</td>
</tr>
<tr>
<td>CIPA</td>
<td>Classified Information Procedures Act</td>
</tr>
<tr>
<td>CKTS</td>
<td>Computerized Key Telephone Systems</td>
</tr>
<tr>
<td>CM</td>
<td>Configuration Management</td>
</tr>
<tr>
<td>CO</td>
<td>Certification Official</td>
</tr>
<tr>
<td>COMSEC</td>
<td>Communications Security</td>
</tr>
<tr>
<td>COOP</td>
<td>Continuity of Operation Plan</td>
</tr>
<tr>
<td>COTR</td>
<td>Contracting Officer Technical Representative</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial-Off-The-Shelf</td>
</tr>
<tr>
<td>CP</td>
<td>Certificate Policy</td>
</tr>
<tr>
<td>CPAU</td>
<td>Clearance Passage and Access Unit</td>
</tr>
<tr>
<td>CPBX</td>
<td>Computerized Private Branch Exchange</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Checking</td>
</tr>
<tr>
<td>CRT</td>
<td>Cathode Ray Tube</td>
</tr>
<tr>
<td>CSA</td>
<td>Cognizant Security Authority</td>
</tr>
<tr>
<td>CSMU</td>
<td>Career Service Management Unit</td>
</tr>
<tr>
<td>CSO</td>
<td>Chief Security Officer</td>
</tr>
<tr>
<td>CSP</td>
<td>Construction Security Plan</td>
</tr>
</tbody>
</table>
CTS: Computerized Telephone Switches
CTTA: Certified TEMPEST Technical Authority
CUA: Co-Utilization Agreement
DAA: Designated Approving Authority
DBA: Data Base Administrator
DCI: Director of Central Intelligence (superceded by Director of National Intelligence)
DCID: Director of Central Intelligence Directive
DCS: Defense Courier Service
DI: Digital Identity
DIA: Defense Intelligence Agency
DIDO: Designated Intelligence Disclosure Officer
DIRNSA: Director, National Security Agency
DJSA: Defense Information Systems Agency
DISCO: Defense Industrial Security Clearance Office
DNI Director of National Intelligence (supercedes title of Director of Central Intelligence)
DOB: Date of Birth
DoD: Department of Defense
DOS: Department of State
DPU: Defensive Programs Unit
DRAM: Dynamic Random Access Memory
DSS: Defense Security Service
DSSCS: Defense Special Security Communications System
DTD: Data Transfer Device
EAL: Evaluation Assurance Level
EAP: Emergency Action Plan
ECC: Evidence Control Center
ECR: Evidence Control Room
ECU: Employee Clearance Unit
ECC: Electronically Erasable Programmable Read-Only Memory
EFLAGS: Register Flags
EPL: Evaluated Products List
EO: Executive Order
EPROM: Erasable Programmable Read-Only Memory
ESOC: Enterprise Security Operations Center
FBI COR: FBI Central Office of Record
FFC: Fixed Facility Checklist
FGI: Foreign Government Information
FISCAM: Federal Information System Controls Audit Manual
FIP: Foreign Integrated Persons
FIP PUB: Federal Information Processing Standards Publication
FISMA: Federal Information Security Management Act
FOCI: Foreign Ownership, Control or Influence
FOUO: For Official Use Only
FSS: Facility Security System
FSU: Facilities Security Unit
G: GAMMA
GSA: General Services Administration
GOTS: Government off the Shelf
GPL: General Public License
GRPU: Government Response/Prepublication Unit
HCO: HUMINT Control Officer
HVAC: Heating Ventilation Air Condition Systems
HVISS: Hirsh Velocity Integrated Security System
IAPC: Information Assurance Policy Council
IATO: Interim Authorization To Operate
IAS: Information Assurance Section
IC: Intelligence Community
IDE: Intrusion Detection Equipment
IDG: Intrusion Detection Group
IDS: Intrusion Detection System
IG: Inspector General
IMINT: Imagery Intelligence
IPMS: In-Place Monitoring System
IS: Information System
ISA: Interconnection Security Agreement
ISD: Inspectable Space Determination
ISOO: Information Security Oversight Office
ISSE: Information System Security Engineering Process
ISSM: Information System Security Manager
ISSO: Information System Security Officer
IT: Information Technology
IOCTL: Input and Output Control
IOP: Privilege levels
IT LCMD: Information Technology Life Cycle Management Directive
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITC</td>
<td>Interagency Training Center</td>
</tr>
<tr>
<td>ITD</td>
<td>Investigative Technology Division</td>
</tr>
<tr>
<td>ITIM</td>
<td>Information Technology Interment Management</td>
</tr>
<tr>
<td>ITOD</td>
<td>Information Technology Operations Division</td>
</tr>
<tr>
<td>JTF</td>
<td>Joint Task Force</td>
</tr>
<tr>
<td>JTTF</td>
<td>Joint Terrorism Task Force</td>
</tr>
<tr>
<td>KVM</td>
<td>Keyboard, Video, Mouse</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LBI</td>
<td>Limited Background Investigation</td>
</tr>
<tr>
<td>LECAU</td>
<td>Law Enforcement Contractor Adjudication Unit</td>
</tr>
<tr>
<td>LFD</td>
<td>Light-Emitting Diode</td>
</tr>
<tr>
<td>LEGATS</td>
<td>Legal Attacheans</td>
</tr>
<tr>
<td>LES</td>
<td>Law Enforcement Sensitive</td>
</tr>
<tr>
<td>LOU</td>
<td>Limited Official Use</td>
</tr>
<tr>
<td>MAC</td>
<td>Mandatory Access Control</td>
</tr>
<tr>
<td>MAOP</td>
<td>Manual of Administrative Operations and Procedures</td>
</tr>
<tr>
<td>MASINT</td>
<td>Measurement and Signature Intelligence</td>
</tr>
<tr>
<td>MIOG</td>
<td>Manual of Investigative Operations and Guidelines</td>
</tr>
<tr>
<td>MLOE</td>
<td>Multiple-level Operating Environments</td>
</tr>
<tr>
<td>MO</td>
<td>Magneto-Optic</td>
</tr>
<tr>
<td>MOA</td>
<td>Memorandum of Agreement</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>MPR</td>
<td>Monthly Progress Report</td>
</tr>
<tr>
<td>NAC</td>
<td>National Agency Check</td>
</tr>
<tr>
<td>NaA</td>
<td>Nondisclosure Agreement</td>
</tr>
<tr>
<td>NFIB</td>
<td>National Foreign Intelligence Board</td>
</tr>
<tr>
<td>NFPA</td>
<td>National Fire Protection Association</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NRO</td>
<td>National Reconnaissance Office</td>
</tr>
<tr>
<td>NSA/CSS</td>
<td>National Security Agency/Central Security Service</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>NSDD</td>
<td>National Security Decision Directive</td>
</tr>
<tr>
<td>NSTISSI</td>
<td>National Security Telecommunications and Information Systems Security Instruction</td>
</tr>
<tr>
<td>NSTISSP</td>
<td>National Security Telecommunications and Information Systems Security Policy</td>
</tr>
<tr>
<td>NSTL</td>
<td>National Security Threat List</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>VIP</td>
<td>Very Important Person</td>
</tr>
<tr>
<td>VOIP</td>
<td>Voice Over Internet Protocol</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Access Point</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
</tbody>
</table>
Appendix C: Legal Authorities

United States Code

- Title 5, US Code, Sections 301, 552, 552a.
- Title 15, US Code, Section 271.
- Title 18, US Code, Sections 531, 1030, 2511, 2703.
- Title 28, US Code, Section 533.
- Title 31, US Code, Section 1301(a).
- Title 47, US Code, Telegraphs, Telephones, and Radiographs, Section 605.
- Title 49, US Code, Section 1472.

Public Laws

- Public Law 107-347, Federal Information System Management Act of 2002 (FISMA)

Code of Federal Regulations

- Title 28, Code of Federal Regulations, Part 17, Classified Information.

Executive Orders

- EO 12656, Assignment of Emergency Responsibilities.
- EO 12968. Access to Classified Information.

Presidential Decision Directive (PDD)

- PDD 39, United States Policy on Counterterrorism.
- PDD 62, Protections Against Unconventional Threats to the Homeland and Americans Overseas.
- PDD 63, Protecting America's Critical Infrastructures, 22 May 1998.

Director of Central Intelligence Directive (DCID)

- Director of Central Intelligence Directive 6/5, Policy for Protection of Certain Non-SCI Sources and Methods Information (SAMI), February 2001.
- DCID 6/6, Security Controls on the Dissemination of Intelligence Information.

Department of Justice (DOJ) Orders

- DOJ Order 960.81, October 26, 1981.
- DOJ Order 1900.7A, Department of Justice Regional Emergency Preparedness Plan.
- DOJ Order 2600.2B, Security Programs and Responsibilities.
UNCLASSIFIED//FOR OFFICIAL USE ONLY

- DOJ Order 2630.4C, Occupant Emergency Program.
- DOJ Order 2640.2E, Information Technology Security.
- DOJ, Justice Management Division, Information Technology Strategic Plan, July 2002.

Department of Defense Regulations

- Department of Defense Instruction 8520.2, Public Key Infrastructure (PKI) and Public Key Enabling, April 1, 2004.

Federal Bureau of Investigation (FBI)


C-3

UNCLASSIFIED//FOR OFFICIAL USE ONLY
UNCLASSIFIED//FOR OFFICIAL USE ONLY


Federal Information Processing Standards (FIPS)

- FIPS, 188, Standard Security Label for Information Transfer.

National Institute of Standards and Technology (NIST)


National Security Telecommunications and Information Systems Security Instruction (NSTISSI) and National Security Telecommunications and Information Systems Security Policy (NSTISSP)

- National Telecommunications and Information Systems Security Policy (NTISSP), No. 11, National Information Assurance Acquisition Policy, January 2000.

Telephone Security Group (TSG)

- TSG Standard 2 (a) (Supplemental), 2001.

Others

UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Federal Preparedness Circular 64, Continuity of the Executive Branch of the Federal Government at the Regional Level During National Security Emergencies.
- General Services Administration (GSA) publication Occupant Emergency Program Guide.
- GSA publication GSA Security Resource Guide.
- Intelligence Community Policy for the Use of Mobile Code in the SCI Environment, 31 May 2002.
- Information Technology Lifecycle Management Directive, September 30, 2005