

# SUMMARY OF FEDERAL CITATIONS FOR THE NATIONAL INSIDER THREAT TASK FORCE

## Table of Contents

<b>United States Code .....</b>	<b>8</b>
• <i>Title 5 U.S. Code § 552a – Records maintained on individuals (Privacy Act of 1974).....</i>	<i>8</i>
• <i>Title 5 U.S. Code § 1304 - Loyalty Investigations; Reports; Revolving Fund (An Act that enacted Title 5, United States Code, “Government Organization and Employees”).....</i>	<i>14</i>
• <i>Title 5 U.S. Code § 3301- Civil Service; Generally (An Act that enacted Title 5, United States Code, “Government Organization and Employees”) .....</i>	<i>15</i>
• <i>Title 5 U.S. Code § 3302 - Competitive service; rules (An Act that enacted Title 5, United States Code, “Government Organization and Employees”) .....</i>	<i>15</i>
• <i>Title 5 U.S. Code § 7311 - Employment Limitations: Loyalty and Striking (An Act that enacted Title 5, United States Code, “Government Organization and Employees”).....</i>	<i>15</i>
• <i>Title 5 U.S. Code § 7312 - Employment Limitations: Employment and Clearance; Individuals Removed for National Security (An Act that enacted Title 5, United States Code, “Government Organization and Employees”) .....</i>	<i>15</i>
• <i>Title 5 U.S. Code § 7313 - Riots and Civil Disorders (An Act that enacted Title 5, United States Code, “Government Organization and Employees”) .....</i>	<i>16</i>
• <i>Title 5 U.S. Code § 7532 - National Security: Suspension and Removal (An Act that enacted Title 5, United States Code, “Government Organization and Employees”).....</i>	<i>16</i>
• <i>Title 5 U.S. Code § 9101- Access to criminal history records for national security and other purposes .....</i>	<i>17</i>
• <i>Title 18 U.S. Code § 2510, et seq. - Interception and disclosure of wire, oral, or electronic communications prohibited (Electronic Communications Privacy Act of 1986) .....</i>	<i>19</i>

• <i>Title 18 U.S. Code § 2701, et seq. – Unlawful Access to Stored Communications (Stored Communications Act)</i> .....	19
• <i>Title 28 U.S. Code § 535 - Investigation of Crimes Involving Government Officers and Employees; Limitations</i> .....	19
• <i>Title 42 U.S. Code § 2000ee-3- Federal agency data mining (The Federal Agency Data Mining Reporting Act of 2007)</i> .....	20
• <i>Title 44 U.S. Code § 3506 - Federal Agency Responsibilities (Paperwork Reduction Act of 1995)</i> .....	22
• <i>Title 44 U.S. Code § 3534 - Federal Agency Responsibilities: Providing Information Security Protections (Federal Information Security Management Act (“FISMA”) of 2002)</i> .....	22
• <i>Title 44 U.S. Code § 3536 - National Security Systems (Federal Information Security Management Act of 2002)</i> .....	23
• <i>Title 44 U.S. Code § 3544 - Federal Agency Responsibilities: Providing Information Security Protections (E-Government Act of 2002)</i> .....	23
• <i>Title 44 U.S. Code § 3546 - Federal Information Security Incident Center (E-Government Act of 2002)</i> .....	24
• <i>Title 44 U.S. Code § 3547 - National Security Systems (E-Government Act of 2002)</i> .....	24
• <i>Title 50 U.S. Code § 402a - Coordination of Counterintelligence Matters with the Federal Bureau of Investigation (Counterintelligence Enhancement Act of 2002)</i> .	25
<b>Code of Federal Regulations</b> .....	<b>27</b>
• <i>Title 5, Code of Federal Regulations (CFR) Part 731 - Suitability for Employment</i> .....	27
• <i>Title 5, CFR, Part 732 - National Security Positions</i> .....	28
• <i>Title 5, CFR, Part 736- Office of Personnel Management, Personnel Investigations</i> .....	28
• <i>Title 32, CFR, Part 147, Subpart B - Investigative Standards</i> .....	29
• <i>Title 32, CFR, Part 2001 - Classified National Security Information</i> .....	31
• <i>Title 41, CFR, Part 102-74 – Facility Management, Subpart C - Conduct on Federal Property</i> .....	33

**Executive Orders.....35**

- EO 13587 - Structural Reforms to Improve the Security of Classified Networks and Responsible Sharing and Safeguarding of Classified Information ..... 35*
- EO 13549 - Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities ..... 37*
- EO 13526 - Classified National Security Information ..... 42*
- EO 13488 - Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust ..... 45*
- EO 13467 - Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information..... 47*
- EO 13286 - Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security..... 50*
- EO 13231 - Critical Infrastructure Protection in the Information Age ..... 51*
- EO 12968 - Access to Classified Information..... 52*
- EO 12829 - National Industrial Security Program ..... 57*
- EO 12564 - Drug-Free Federal Workplace ..... 58*
- EO 12333 - United States Intelligence Activities (as amended by Executive Orders 13284 (2003), 13355 (2004), and 13470 (2008)) ..... 63*
- EO 10577 - Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service ..... 64*
- EO 10450 - Security Requirements for Government Employment (See generally Title 5 US Code § 7311: Employment Limitations, Loyalty and Striking) ..... 68*

**Presidential National Security Directives and Homeland Security Presidential Directives.....71**

- National Security Directive 42 - National Policy for the Security of National Security Telecommunications and Information Systems..... 71*
- National Security Directive 63 - Single Scope Background Investigations ..... 71*

• <i>Presidential Decision Directive/NSC-12- Security Awareness and Reporting of Foreign Contacts</i> .....	73
• <i>National Security Presidential Directive 54/Homeland Security Presidential Directive 23 - Cybersecurity Policy</i> .....	74
• <i>Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience</i> .....	74
• <i>Homeland Security Presidential Directive 12 - Policies for a Common Identification Standard for Federal Employees and Contractors</i> .....	74
<b>Intelligence Community Directives .....</b>	<b>75</b>
• <i>Intelligence Community Directive 500 – Chief Information Officer</i> .....	75
• <i>Intelligence Community Directive 503 - Information Technology Systems Security, Risk Management, Certification and Accreditation</i> .....	75
• <i>Intelligence Community Directive 700 - Protection of National Intelligence</i> .....	76
• <i>Intelligence Community Directive 704 - Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information</i> .....	77
• <i>Intelligence Community Directive 705 - Sensitive Compartmented Information Facilities</i>	78
<b>Intelligence Community Standards.....</b>	<b>79</b>
• <i>Intelligence Community Standard Number 700-2 – Use of Audit Data for Insider Threat Detection (Effective June 2, 2011)</i> .....	79
<b>Miscellaneous References .....</b>	<b>80</b>
Memorandum of Understanding (“MOU”): Reporting of Information Concerning Federal Crimes (signed by Intelligence Community agencies in 1995).....	80
MOU between the FBI and EPA RE 811 Referrals, dated July 11, 2012. ....	80
U.S. Department of Justice, Office of Legal Counsel, MEMORANDUM OPINION FOR AN ASSOCIATE DEPUTY ATTORNEY GENERAL, “Legality of Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch,” August 14, 2009.....	80

U.S. Department of Justice, Office of Legal Counsel, MEMORANDUM OPINION FOR THE COUNSEL TO THE PRESIDENT, “Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch,” January 9, 2009.....	80
White House Memorandum, “Early Detection of Espionage and Other Intelligence Activities Through the Identification and Referral of Anomalies,” August 23, 1996.....	80
Presidential Memorandum for the Heads of Executive Departments and Agencies, “National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs,” dated November 21, 2012.....	80
U.S. Department of Justice Memorandum for the Attorney General from the Office of the Deputy Attorney General RE WARRANTLESS SEARCHES OF DOJ EMPLOYEES WITH ACCESS TO CLASSIFIED INFORMATION, October 15, 2001.....	80
Office of Management and Budget (“OMB”) Circular No. A-130, Management of Federal Information Resources, Appendix III - Security of Federal Automated Information Resources.....	80
MEMORANDUM FOR EXECUTIVE DEPARTMENTS AND AGENCIES from U.S. Office of Special Counsel, Special Counsel Carolyn N. Lerner, RE Agency Monitoring Policies and Confidential Whistleblower Disclosures to the Office of Special Counsel and to Inspectors General, dated June 20, 2012. ....	80
ATTORNEY GENERAL GUIDELINES FOR OFFICES OF INSPECTOR GENERAL WITH STATUTORY LAW ENFORCEMENT AUTHORITY, dated December 8, 2005..	80
Federal Register/Vol. 70, No. 29/Page 7513, Monday, February 14, 2005/Notices: Provides <i>Notice</i> concerning the routine uses of records maintained in the Federal Bureau of Investigation’s System of Records under the Privacy Act).....	80
66 FR 33559, June 22, 2001, Blanket Routine Uses Applicable to More Than One FBI Privacy Act System of Records. ....	80
72 FR 3410, January 25, 2007, <i>DOJ Blanket Routine Use Authorizing Disclosure of Information in Response to a Data Breach</i> . ....	81
63 FR 8671, 8682, February 20, 1998, <i>Privacy Act System of Records Notice for the FBI Central Records System</i> . ....	81
MEMORANDUM FOR HEADS OF DEPARTMENTS AND AGENCIES, CHIEF HUMAN CAPITAL OFFICERS, AND AGENCY SECURITY OFFICERS, FROM: LINDA M. SPRINGER, DIRECTOR OF THE UNITED STATES OFFICE OF	

PERSONNEL MANAGEMENT, SUBJECT: Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide, January 14, 2008.....	81
DoD Instruction O-5240.21, “Counterintelligence (CI) Inquiries,” May 14, 2009.....	81
U.S. Department of Homeland Security, Privacy Impact Assessment for EINSTEIN 3 – Accelerated (E <sup>3</sup> A), April 19, 2013. ( <b>Abstract:</b> The Department of Homeland Security (DHS), Office of Cybersecurity and Communications (CS&C) continues to improve its ability to defend federal civilian Executive Branch agency networks from cyber threats. Similar to EINSTEIN 1 and EINSTEIN 2, DHS will deploy EINSTEIN 3 Accelerated (E3A) to enhance cybersecurity analysis, situational awareness, and security response. With E3A, DHS will not only be able to detect malicious traffic targeting federal government networks, but also prevent malicious traffic from harming those networks. This will be accomplished through delivering intrusion prevention capabilities as a Managed Security Service provided by Internet Service Providers (ISP). Under the direction of DHS, ISPs will administer intrusion prevention and threat-based decision-making on network traffic entering and leaving participating federal civilian Executive Branch agency networks.....	81
<b>Forms.....</b>	<b>81</b>
SF-75 (Request for Preliminary Employment Data) .....	81
SF-86 (EO10450 Questionnaire for National Security Positions); .....	81
SF 85 (Questionnaire for Nonsensitive Positions); .....	82
SF 85P (Questionnaire for Public Trust Positions); .....	82
SF-86A (Continuation Form for SF-86, SF-85, and SF-85P); .....	82
SF-312 (Classified Information Nondisclosure Agreement).....	82
OF 306 (Declaration for Federal Employment); .....	82
OGE Forms 450, 278, 278T (Ethics Financial Disclosure Forms) .....	82
SF-713 (EO-12968 Consent to Access to Records); .....	82
Form 4414 (EF) (Sensitive Compartmented Information Nondisclosure Agreement); .....	82
FD-328 (Consent to Polygraph) .....	82
FD-857 (Sensitive Information Nondisclosure Agreement); .....	82

FD-868 (Nondisclosure Agreement for Joint Task Force Members, Contractors, Detailees, Assignees, and Interns);.....	82
FD-889 (IT Systems Use Agreement);.....	82
FD-979 (Personnel Consent to Release Information).....	82
EO- 12564 (Drug-Free Federal Workplace) - (No specific federal forms. The testing requirement is found within specified "Position Descriptions" for pre-employment, random, and "for cause" employee drug screening) .....	82
DOJ-555 (Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act (Title 15, U.S. Code, Section 1681)).....	82

## **United States Code**

### **•Title 5 U.S. Code § 552a – Records maintained on individuals (Privacy Act of 1974)**

**(a) Definitions.**--For purposes of this section--

(1) the term "agency" means agency as defined in section 552(e) of this title;

(2) the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence;

(3) the term "maintain" includes maintain, collect, use, or disseminate;

(4) the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;

(5) the term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;

(6) the term "statistical record" means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13;

(7) the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected;

(8) the term "matching program"--

**(A)** means any computerized comparison of--

(i) two or more automated systems of records or a system of records with non-Federal records for the purpose of--

(I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or

(II) recouping payments or delinquent debts under such Federal benefit programs, or

(ii) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records,

**(B)** but does not include--



- (i) matches performed to produce aggregate statistical data without any personal identifiers;
- (ii) matches performed to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals;
- (iii) matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons;
- (iv) matches of tax information (I) pursuant to section 6103(d) of the Internal Revenue Code of 1986, (II) for purposes of tax administration as defined in section 6103(b)(4) of such Code, (III) for the purpose of intercepting a tax refund due an individual under authority granted by section 404(e), 464, or 1137 of the Social Security Act; or (IV) for the purpose of intercepting a tax refund due an individual under any other tax refund intercept program authorized by statute which has been determined by the Director of the Office of Management and Budget to contain verification, notice, and hearing requirements that are substantially similar to the procedures in section 1137 of the Social Security Act;
- (v) matches--
  - (I) using records predominantly relating to Federal personnel, that are performed for routine administrative purposes (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)); or
  - (II) conducted by an agency using only records from systems of records maintained by that agency;
    - if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel;
- (vi) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel;
- (vii) matches performed incident to a levy described in section 6103(k)(8) of the Internal Revenue Code of 1986;
- (viii) matches performed pursuant to section 202(x)(3) or 1611(e)(1) of the Social Security Act (42 U.S.C. 402(x)(3), 1382(e)(1)); or
- (ix) matches performed by the Secretary of Health and Human Services or the Inspector General of the Department of Health and Human Services with respect to potential fraud, waste, and abuse, including matches of a system of records with non-Federal records;
- (9) the term "recipient agency" means any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program;
- (10) the term "non-Federal agency" means any State or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a matching program;

(11) the term "source agency" means any agency which discloses records contained in a system of records to be used in a matching program, or any State or local government, or agency thereof, which discloses records to be used in a matching program;

(12) the term "Federal benefit program" means any program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals; and

(13) the term "Federal personnel" means officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals [FN1] entitled to receive immediate or deferred retirement benefits under any retirement program of the Government of the United States (including survivor benefits).

**(b) Conditions of disclosure.**--No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be--

(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

(2) required under section 552 of this title;

(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;

(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

(6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;

(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

(10) to the Comptroller General, or any of his authorized representatives, in the course of the

performance of the duties of the Government Accountability Office;

(11) pursuant to the order of a court of competent jurisdiction; or

(12) to a consumer reporting agency in accordance with section 3711(e) of title 31.

**(c) Accounting of certain disclosures.**--Each agency, with respect to each system of records under its control, shall--

(1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of--

(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

(B) the name and address of the person or agency to whom the disclosure is made;

(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

(3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

**(d) Access to records.**--Each agency that maintains a system of records shall--

(1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;

(2) permit the individual to request amendment of a record pertaining to him and--

(A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and

(B) promptly, either--

(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;

(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a

final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;

(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

**(e) Agency requirements.**--Each agency that maintains a system of records shall--

(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual--

(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

(B) the principal purpose or purposes for which the information is intended to be used;

(C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and

(D) the effects on him, if any, of not providing all or any part of the requested information;

**(j) General exemptions.**--The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is--

(1) maintained by the Central Intelligence Agency; or

(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of

identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

**(k) Specific exemptions.**--The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is--

(1) subject to the provisions of section 552(b)(1) of this title;

(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: *Provided, however,* That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18;

(4) required by statute to be maintained and used solely as statistical records;

(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a

provision of this section.

(Writer's note: *See e.g.*, Federal Register/Vol. 70, No. 29/Page 7513, Monday, February 14, 2005/Notices: Provides *Notice* concerning the routine uses of records maintained in the Federal Bureau of Investigation's System of Records under the Privacy Act).

**•Title 5 U.S. Code § 1304 - Loyalty Investigations; Reports; Revolving Fund (An Act that enacted Title 5, United States Code, "Government Organization and Employees")**

(a) The Office of Personnel Management shall conduct the investigations and issue the reports required by the following statutes--

- (1) [sections 272b, 281b\(e\), and 290a of title 22;](#)
- (2) [section 1874\(c\) of title 42;](#) and
- (3) [section 1203\(e\) of title 6,](#) District of Columbia Code.

(b) When an investigation under subsection (a) of this section develops data indicating that the loyalty of the individual being investigated is questionable, the Office shall refer the matter to the Federal Bureau of Investigation for a full field investigation, a report of which shall be furnished to the Office for its information and appropriate action.

(c) When the President considers it in the national interest, he may have the investigations of a group or class, which are required by subsection (a) of this section, made by the Federal Bureau of Investigation rather than the Office.

(d) The investigation and report required by subsection (a) of this section shall be made by the Federal Bureau of Investigation rather than the Office for those specific positions which the Secretary of State certifies are of a high degree of importance or sensitivity.

(e) The Comptroller General of the United States shall, as a result of his periodic reviews of the activities financed by the fund, report and make such recommendations as he deems appropriate to the Committee on Governmental Affairs of the Senate and the Committee on Post Office and Civil Service of the House of Representatives.

(f) An agency may use available appropriations to reimburse the Office or the Federal Bureau of Investigation for the cost of investigations, training, and functions performed for them under this section, or to make advances toward their cost. These advances and reimbursements shall be credited directly to the applicable appropriations of the Office or the Federal Bureau of Investigation.

(g) This section does not affect the responsibility of the Federal Bureau of Investigation to investigate espionage, sabotage, or subversive acts.

• ***Title 5 U.S. Code § 3301- Civil Service; Generally (An Act that enacted Title 5, United States Code, “Government Organization and Employees”)***

The President may--

- (1) prescribe such regulations for the admission of individuals into the civil service in the executive branch as will best promote the efficiency of that service;
- (2) ascertain the fitness of applicants as to age, health, character, knowledge, and ability for the employment sought; and
- (3) appoint and prescribe the duties of individuals to make inquiries for the purpose of this section.

• ***Title 5 U.S. Code § 3302 - Competitive service; rules (An Act that enacted Title 5, United States Code, “Government Organization and Employees”)***

The President may prescribe rules governing the competitive service. The rules shall provide, as nearly as conditions of good administration warrant, for--

- (1) necessary exceptions of positions from the competitive service; and
- (2) necessary exceptions from the provisions of [sections 2951](#), [3304\(a\)](#), [3321](#), [7202](#), and [7203](#) of this title.

Each officer and individual employed in an agency to which the rules apply shall aid in carrying out the rules.

• ***Title 5 U.S. Code § 7311 - Employment Limitations: Loyalty and Striking (An Act that enacted Title 5, United States Code, “Government Organization and Employees”)***

An individual may not accept or hold a position in the Government of the United States or the government of the District of Columbia if he--

- (1) advocates the overthrow of our constitutional form of government;
- (2) is a member of an organization that he knows advocates the overthrow of our constitutional form of government;
- (3) participates in a strike, or asserts the right to strike, against the Government of the United States or the government of the District of Columbia; or
- (4) is a member of an organization of employees of the Government of the United States or of individuals employed by the government of the District of Columbia that he knows asserts the right to strike against the Government of the United States or the government of the District of Columbia.

• ***Title 5 U.S. Code § 7312 - Employment Limitations: Employment and Clearance; Individuals Removed for National Security (An Act that enacted Title 5, United States Code, “Government Organization and Employees”)***

Removal under [section 7532](#) of this title does not affect the right of an individual so removed to seek or accept employment in an agency of the United States other than the agency from which removed. However, the appointment of an individual so removed may be made only after the head of the agency concerned has consulted with the Office of Personnel Management. The Office, on written request of the

head of the agency or the individual so removed, may determine whether the individual is eligible for employment in an agency other than the agency from which removed.

• ***Title 5 U.S. Code § 7313 - Riots and Civil Disorders (An Act that enacted Title 5, United States Code, "Government Organization and Employees")***

(a) An individual convicted by any Federal, State, or local court of competent jurisdiction of--

- (1) inciting a riot or civil disorder;
- (2) organizing, promoting, encouraging, or participating in a riot or civil disorder;
- (3) aiding or abetting any person in committing any offense specified in clause (1) or (2);
- or
- (4) any offense determined by the head of the employing agency to have been committed in furtherance of, or while participating in, a riot or civil disorder;

shall, if the offense for which he is convicted is a felony, be ineligible to accept or hold any position in the Government of the United States or in the government of the District of Columbia for the five years immediately following the date upon which his conviction becomes final. Any such individual holding a position in the Government of the United States or the government of the District of Columbia on the date his conviction becomes final shall be removed from such position.

(b) For the purposes of this section, "felony" means any offense for which imprisonment is authorized for a term exceeding one year.

• ***Title 5 U.S. Code § 7532 - National Security: Suspension and Removal (An Act that enacted Title 5, United States Code, "Government Organization and Employees")***

(a) Notwithstanding other statutes, the head of an agency may suspend without pay an employee of his agency when he considers that action necessary in the interests of national security. To the extent that the head of the agency determines that the interests of national security permit, the suspended employee shall be notified of the reasons for the suspension. Within 30 days after the notification, the suspended employee is entitled to submit to the official designated by the head of the agency statements or affidavits to show why he should be restored to duty.

(b) Subject to subsection (c) of this section, the head of an agency may remove an employee suspended under subsection (a) of this section when, after such investigation and review as he considers necessary, he determines that removal is necessary or advisable in the interests of national security. The determination of the head of the agency is final.

(c) An employee suspended under subsection (a) of this section who--

- (1) has a permanent or indefinite appointment;
- (2) has completed his probationary or trial period; and
- (3) is a citizen of the United States



• *Title 5 U.S. Code § 9101- Access to criminal history records for national security and other purposes*

(a) As used in this section:

(1) The term "criminal justice agency" means (A) any Federal, State, or local court, and (B) any Federal, State, or local agency, or any subunit thereof, which performs the administration of criminal justice pursuant to a statute or Executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice.

(2) The term "criminal history record information" means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, sentencing, correction supervision, and release. The term does not include identification information such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system. The term does not include those records of a State or locality sealed pursuant to law from access by State and local criminal justice agencies of that State or locality.

(3) The term "classified information" means information or material designated pursuant to the provisions of a statute or Executive order as requiring protection against unauthorized disclosure for reasons of national security.

(4) The term "State" means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, Guam, the Virgin Islands, American Samoa, and any other territory or possession of the United States.

(5) The term "local" and "locality" means any local government authority or agency or component thereof within a State having jurisdiction over matters at a county, municipal, or other local government level.

(6) The term "covered agency" means any of the following:

(A) The Department of Defense.

(B) The Department of State.

(C) The Department of Transportation.

(D) The Office of Personnel Management.

(E) The Central Intelligence Agency.

(F) The Federal Bureau of Investigation.

(b)(1) Upon request by the head of a covered agency, criminal justice agencies shall make available criminal history record information regarding individuals under investigation by that covered agency for the purpose of determining eligibility for any of the following:

(A) Access to classified information.

(B) Assignment to or retention in sensitive national security duties.

(C) Acceptance or retention in the armed forces.

(D) Appointment, retention, or assignment to a position of public trust or a critical or sensitive position while either employed by the Government or performing a Government contract.

(2) Such a request to a State central criminal history record repository shall be accompanied by the fingerprints of the individual who is the subject of the request if required by State law and if the repository uses the fingerprints in an automated fingerprint identification system.

(3) Fees, if any, charged for providing criminal history record information pursuant to this subsection shall not exceed the reasonable cost of providing such information.

(4) This subsection shall apply notwithstanding any other provision of law or regulation of any State or of any locality within a State, or any other law of the United States.

(c) A covered agency shall not obtain criminal history record information pursuant to this section unless it has received written consent from the individual under investigation for the release of such information for the purposes set forth in paragraph (b)(1).

(d) Criminal history record information received under this section shall be disclosed or used only for the purposes set forth in paragraph (b)(1) or for national security or criminal justice purposes authorized by law, and such information shall be made available to the individual who is the subject of such information upon request.

(e)(1) Automated information delivery systems shall be used to provide criminal history record information to a covered agency under subsection (b) whenever available.

(2) Fees, if any, charged for automated access through such systems may not exceed the reasonable cost of providing such access.

(3) The criminal justice agency providing the criminal history record information through such systems may not limit disclosure on the basis that the repository is accessed from outside the State.

(4) Information provided through such systems shall be the full and complete criminal history record.

(5) Criminal justice agencies shall accept and respond to requests for criminal history record information through such systems with printed or photocopied records when requested.

(f) The authority provided under this section with respect to the Department of State may be exercised only so long as the Department of State continues to extend to its employees and applicants for employment, at a minimum, those procedural safeguards provided for as part of the security clearance process that were made available, as of May 1, 1987, pursuant to section 163.4 of volume 3 of the Foreign Affairs Manual.

• ***Title 18 U.S. Code § 2510, et seq. - Interception and disclosure of wire, oral, or electronic communications prohibited (Electronic Communications Privacy Act of 1986)***

(Writers's note: Title III of the Electronic Communications Privacy Act ("ECPA") governs live "wire," "oral," and "electronic" communications. This Act has a consent provision that U.S. government agencies can rely on in crafting banners/user agreements to get consent from employees to search their historical records and to monitor their communications).

• ***Title 18 U.S. Code § 2701, et seq. – Unlawful Access to Stored Communications (Stored Communications Act)***

(Writer's note: Federal courts have interpreted the Stored Communications Act ("SCA") to include any entities that allow their users to communicate with the public, e.g., FBI employees using UNET. The SCA governs stored and historical records. This Act has a consent provision that U.S. government agencies can rely on in crafting banners/user agreements to obtain consent from employees to search their historical records, and, to monitor their communications).

• ***Title 28 U.S. Code § 535 - Investigation of Crimes Involving Government Officers and Employees; Limitations***

*\*\*Note the reporting requirement by head of each department or agency regarding violations of Federal criminal laws to the Attorney General.*

(a) The Attorney General and the Federal Bureau of Investigation may investigate any violation of Federal criminal law involving Government officers and employees--

(1) notwithstanding any other provision of law; and

(2) without limiting the authority to investigate any matter which is conferred on them or on a department or agency of the Government.

(b) Any information, allegation, matter, or complaint witnessed, discovered, or received in a department or agency of the executive branch of the Government relating to violations of Federal criminal law involving Government officers and employees shall be expeditiously reported to the

Attorney General by the head of the department or agency, or the witness, discoverer, or recipient, as appropriate, unless--

(1) the responsibility to perform an investigation with respect thereto is specifically assigned otherwise by another provision of law; or

(2) as to any department or agency of the Government, the Attorney General directs otherwise with respect to a specified class of information, allegation, or complaint.

(c) This section does not limit--

(1) the authority of the military departments to investigate persons or offenses over which the armed forces have jurisdiction under the Uniform Code of Military Justice (chapter 47 of title 10); or

(2) the primary authority of the Postmaster General to investigate postal offenses.

• ***Title 42 U.S. Code § 2000ee-3- Federal agency data mining (The Federal Agency Data Mining Reporting Act of 2007)***

(a) Short title -- This section may be cited as the "Federal Agency Data Mining Reporting Act of 2007".

(b) Definitions -- in this section:

(1) Data mining

The term "data mining" means a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where--

**(A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;**

**(B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and**

**(C) the purpose of the queries, searches, or other analyses is not solely--**

**(i) the detection of fraud, waste, or abuse in a Government agency or program; or**

**(ii) the security of a Government computer system.**

(2) Database

The term "database" does not include telephone directories, news reporting, information publicly available to any member of the public without payment of a fee, or databases of judicial and administrative opinions or other legal research sources.

(c) Reports on data mining activities by Federal agencies

(1) Requirement for report

The head of each department or agency of the Federal Government that is engaged in any activity to use or develop data mining shall submit a report to Congress on all such activities of the department or agency under the jurisdiction of that official. The report shall be produced in coordination with the privacy officer of that department or agency, if applicable, and shall be made available to the public, except for an annex described in subparagraph (C).

(2) Content of report

Each report submitted under subparagraph (A) shall include, for each activity to use or develop data mining, the following information:

(A) A thorough description of the data mining activity, its goals, and, where appropriate, the target dates for the deployment of the data mining activity.

(B) A thorough description of the data mining technology that is being used or will be used, including the basis for determining whether a particular pattern or anomaly is indicative of terrorist or criminal activity.

(C) A thorough description of the data sources that are being or will be used.

(D) An assessment of the efficacy or likely efficacy of the data mining activity in providing accurate information consistent with and valuable to the stated goals and plans for the use or development of the data mining activity.

(E) An assessment of the impact or likely impact of the implementation of the data mining activity on the privacy and civil liberties of individuals, including a thorough description of the actions that are being taken or will be taken with regard to the property, privacy, or other rights or privileges of any individual or individuals as a result of the implementation of the data mining activity.

(F) A list and analysis of the laws and regulations that govern the information being or to be collected, reviewed, gathered, analyzed, or used in conjunction with the data mining activity, to the extent applicable in the context of the data mining activity.

(G) A thorough discussion of the policies, procedures, and guidelines that are in place or that are to be developed and applied in the use of such data mining activity in order to--

(i) protect the privacy and due process rights of individuals, such as redress procedures; and

(ii) ensure that only accurate and complete information is collected, reviewed, gathered, analyzed, or used, and guard against any harmful consequences of potential inaccuracies.

(3) Annex

(A) In general

A report under subparagraph (A) shall include in an annex any necessary--

- (i) classified information;
- (ii) law enforcement sensitive information;
- (iii) proprietary business information; or
- (iv) trade secrets (as that term is defined in section 1839 of Title 18).

(B) Availability

Any annex described in clause (i)--

(i) shall be available, as appropriate, and consistent with the National Security Act of 1947 (50 U.S.C. 401 et seq.), to the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Select Committee on Intelligence, the Committee on Appropriations, and the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Homeland Security, the Committee on the Judiciary, the Permanent Select Committee on Intelligence, the Committee on Appropriations, and the Committee on Financial Services of the House of Representatives; and

(ii) shall not be made available to the public.

(4) Time for report -- Each report required under subparagraph (A) shall be--

(A) submitted not later than 180 days after August 3, 2007; and

(B) updated not less frequently than annually thereafter, to include any activity to use or develop data mining engaged in after the date of the prior report submitted under subparagraph (A).

• ***Title 44 U.S. Code § 3506 - Federal Agency Responsibilities (Paperwork Reduction Act of 1995)***

(g) With respect to privacy and security, each agency shall--

(1) implement and enforce applicable policies, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for the agency; and

(2) assume responsibility and accountability for compliance with and coordinated management of [sections 552 and 552a of title 5](#), subchapter II of this chapter, and related information management laws.

[(3) Repealed. [Pub.L. 107-296, Title X, § 1005\(c\)\(3\)\(C\)](#), Nov. 25, 2002, 116 Stat. 2273]

(h) With respect to Federal information technology, each agency shall--

(1) implement and enforce applicable Government wide and agency information technology management policies, principles, standards, and guidelines.

• ***Title 44 U.S. Code § 3534 - Federal Agency Responsibilities: Providing Information Security Protections (Federal Information Security Management Act ("FISMA") of 2002)***

*\*\*Note FISMA was enacted as part of the E-Government Act of 2002.*

(a) The head of each agency shall--

(1) be responsible for--

(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of--

(i) information collected or maintained by or on behalf of the agency;  
and

(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including--

(i) information security standards promulgated by the Director under [section 11331 of title 40](#); and

(ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes.

• ***Title 44 U.S. Code § 3536 - National Security Systems (Federal Information Security Management Act of 2002)***

The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency--

(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;

(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

(3) complies with the requirements of this subchapter.

• ***Title 44 U.S. Code § 3544 - Federal Agency Responsibilities: Providing Information Security Protections (E-Government Act of 2002)***

(a) **In general.**--The head of each agency shall--

(1) be responsible for--

(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of--

(i) information collected or maintained by or on behalf of the agency;  
and

- (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;
- (B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including--
  - (i) information security standards promulgated under [section 11331 of title 40](#); and
  - (ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and
- (C) ensuring that information security management processes are integrated with agency strategic and operational planning processes;
- (2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through--
  - (A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;
  - (B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under [section 11331 of title 40](#), for information security classifications and related requirements;
  - (C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and
  - (D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented.

• ***Title 44 U.S. Code § 3546 - Federal Information Security Incident Center (E-Government Act of 2002)***

**(b) National security systems.**--Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

• ***Title 44 U.S. Code § 3547 - National Security Systems (E-Government Act of 2002)***

The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency--

- (1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;
- (2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and
- (3) complies with the requirements of this subchapter.



• ***Title 50 U.S. Code § 402a - Coordination of Counterintelligence Matters with the Federal Bureau of Investigation (Counterintelligence Enhancement Act of 2002) .***

*\*\*Note the reporting requirement: The head of each department or agency within the executive branch shall ensure that the Federal Bureau of Investigation is advised immediately of any information, regardless of its origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power.*

*\*\*Also note: In Title 50, United States Code, chapter 15 is being reorganized into four new chapters in order to set forth more clearly the provisions of the National Security Act of 1947, the Central Intelligence Agency Act of 1949, the National Security Agency Act of 1959, and certain other related statutes. No statutory text is altered by this action. The provisions are merely being transferred from one place to another in Title 50, United States Code. Effective May 20, 2013, Title 50 U.S. Code § 402a will be transferred to new section number 3381.*

**(e) Coordination of counterintelligence matters with Federal Bureau of Investigation**

(1) Except as provided in paragraph (5), the head of each department or agency within the executive branch shall ensure that--

(A) the Federal Bureau of Investigation is advised immediately of any information, regardless of its origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power;

(B) following a report made pursuant to subparagraph (A), the Federal Bureau of Investigation is consulted with respect to all subsequent actions which may be undertaken by the department or agency concerned to determine the source of such loss or compromise; and

(C) where, after appropriate consultation with the department or agency concerned, the Federal Bureau of Investigation undertakes investigative activities to determine the source of the loss or compromise, the Federal Bureau of Investigation is given complete and timely access to the employees and records of the department or agency concerned for purposes of such investigative activities.

(2) Except as provided in paragraph (5), the Director of the Federal Bureau of Investigation shall ensure that espionage information obtained by the Federal Bureau of Investigation pertaining to the personnel, operations, or information of departments or agencies of the executive branch, is provided through appropriate channels in a timely manner to the department or agency concerned, and that such departments or agencies are consulted in a timely manner with respect to espionage investigations undertaken by the Federal Bureau of Investigation which involve the personnel, operations, or information of such department or agency.

(3)(A) The Director of the Federal Bureau of Investigation shall submit to the head of the department or agency concerned a written assessment of the potential impact of the actions of the department or agency on a counterintelligence investigation.

(B) The head of the department or agency concerned shall

(i) use an assessment under subparagraph (A) as an aid in determining whether, and under what circumstances, the subject of an investigation under paragraph (1) should be left in place for investigative purposes; and

(ii) notify in writing the Director of the Federal Bureau of Investigation of such determination.

(C) The Director of the Federal Bureau of Investigation and the head of the department or agency concerned shall continue to consult, as appropriate, to review the status of an investigation covered by this paragraph, and to reassess, as appropriate, a determination of the head of the department or agency concerned to leave a subject in place for investigative purposes.

(4)(A) The Federal Bureau of Investigation shall notify appropriate officials within the executive branch, including the head of the department or agency concerned, of the commencement of a full field espionage investigation with respect to an employee within the executive branch.

(B) A department or agency may not conduct a polygraph examination, interrogate, or otherwise take any action that is likely to alert an employee covered by a notice under subparagraph (A) of an investigation described in that subparagraph without prior coordination and consultation with the Federal Bureau of Investigation.

(5) Where essential to meet extraordinary circumstances affecting vital national security interests of the United States, the President may on a case-by-case basis waive the requirements of paragraph (1), (2), or (3), as they apply to the head of a particular department or agency, or the Director of the Federal Bureau of Investigation. Such waiver shall be in writing and shall fully state the justification for such waiver. Within thirty days, the President shall notify the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives that such waiver has been issued, and at that time or as soon as national security considerations permit, provide these committees with a complete explanation of the circumstances which necessitated such waiver.

(6) Nothing in this section may be construed to alter the existing jurisdictional arrangements between the Federal Bureau of Investigation and the Department of Defense with respect to investigations of persons subject to the Uniform Code of Military Justice, nor to impose additional reporting requirements upon the Department of Defense with respect to such investigations beyond those required by existing law and executive branch policy.

(7) As used in this section, the terms "foreign power" and "agent of a foreign power" have the same meanings as set forth in sections [\[FN1\]](#) 1801(a) and (b), respectively, of this title.

## **Code of Federal Regulations**

### **•Title 5, Code of Federal Regulations (CFR) Part 731 - Suitability for Employment**

#### **§ 731.101 Purpose.**

(a) The purpose of this part is to establish criteria and procedures for making determinations of suitability and for taking suitability actions regarding employment in covered positions (as defined in paragraph (b) of this section) pursuant to [5 U.S.C. 3301](#), [E.O. 10577 \(3 CFR, 1954–1958 Comp., p. 218\)](#), as amended, and [5 CFR 1.1, 2.1\(a\)](#) and [5.2](#). [Section 3301 of title 5, United States Code](#), directs consideration of “age, health, character, knowledge, and ability for the employment sought.” [E.O. 10577](#) (codified in relevant part at [5 CFR 1.1, 2.1\(a\)](#) and [5.2](#)) directs OPM to examine “suitability” for competitive Federal employment. This part concerns only determinations of “suitability,” that is, those determinations based on a person's character or conduct that may have an impact on the integrity or efficiency of the service. Determinations made and actions taken under this part are distinct from objections to eligibles or pass overs of preference eligibles, and OPM's and agencies' decisions on such requests, made under [5 U.S.C. 3318](#) and [5 CFR 332.406](#), as well as determinations of eligibility for assignment to, or retention in, sensitive national security positions made under [E.O. 10450 \(3 CFR, 1949–1953 Comp., p. 936\)](#), [E.O. 12968](#), or similar authorities.

(b) Definitions. In this part:

Applicant means a person who is being considered or has been considered for employment.

Appointee means a person who has entered on duty and is in the first year of a subject-to-investigation appointment (as defined in [§ 731.104](#)).

Core Duty means a continuing responsibility that is of particular importance to the relevant covered position or the achievement of an agency's mission.

Covered position means a position in the competitive service, a position in the excepted service where the incumbent can be noncompetitively converted to the competitive service, and a career appointment to a position in the Senior Executive Service.

Days means calendar days unless otherwise specified in this part.

Employee means a person who has completed the first year of a subject-to-investigation appointment.

Material means, in reference to a statement, one that is capable of influencing, affects, or has a natural tendency to affect, an official decision even if OPM or an agency does not rely upon it.

Suitability action means an outcome described in [§ 731.203](#) and may be taken only by OPM or an agency with delegated authority under the procedures in subparts C and D of this part.

Suitability determination means a decision by OPM or an agency with delegated authority that a person is suitable or is not suitable for employment in covered positions in the Federal Government or a specific Federal agency.

[[73 FR 66492](#), Nov. 10, 2008]

•*Title 5, CFR, Part 732 - National Security Positions*

**§ 732.101 Purpose.**

This part sets forth certain requirements and procedures which each agency shall observe for determining national security positions pursuant to [Executive Order 10450--Security Requirements for Government Employment \(April 27, 1953\)](#), 18 FR 2489, 3 CFR 1949–1953 Comp., p. 936, as amended.

SOURCE: [56 FR 18654](#), April 23, 1991, unless otherwise noted.

AUTHORITY: [5 U.S.C. 3301](#), [3302](#), [7312](#); [50 U.S.C. 403](#); [E.O. 10450](#); 3 CFR 1949–1953 Comp., p. 936.

•*Title 5, CFR, Part 736- Office of Personnel Management, Personnel Investigations*

**§ 736.101 Purpose and definitions.**

(a) Purpose. The purpose of this part is to specify certain requirements for personnel investigations conducted by OPM, and for those conducted under delegated authority from OPM. The requirements of this part apply to suitability and national security investigations conducted under parts 731 and 732 of this chapter; they also apply to investigations to determine eligibility or qualifications not covered in parts 731 and 732 of this chapter. The requirements of this part apply to employees in the civil service of the Executive Branch and to persons performing contract, voluntary or indirect services for the Federal Government, as set forth in subsection (b) below.

(b) Definitions. For the purposes of this part,

(1) Federal employment includes the following range of services performed for the Federal government: (i) All employment in the competitive or excepted service or the Senior Executive Service in the Executive Branch; (ii) appointments, salaried or unsalaried, to Federal Advisory Committees or to membership agencies; (iii) cooperative work assignments in which the individual has access to Federal materials such as examination booklets, or performs service for, or under supervision of, a Federal agency while being paid by another organization such as a State or local government; (iv) volunteer arrangements in which the individual performs service for, or under the supervision of, a Federal agency; and (v) volunteer or other arrangements in which the individual represents the United States Government or any agency thereof.

(2) Agency means any authority of the Government of the United States, whether or not it is within or subject to review by another agency, and includes any executive department, military department, Government corporation, Government-controlled corporation, or other establishment in the executive branch of the Government, or any independent regulatory agency.

(3) Personnel investigation means an investigation conducted by written or telephone inquiries or through personal contacts to determine the suitability, eligibility, or qualifications of individuals for Federal employment, for work on Federal contracts, or for access to classified information or restricted areas.

SOURCE: [56 FR 18655](#), April 23, 1991, unless otherwise noted. AUTHORITY: [Pub.L. 93–579](#);

([5 U.S.C. 552a](#)).

•***Title 32, CFR, Part 147, Subpart B - Investigative Standards***

Code of Federal Regulations

**Title 32.** National Defense

Subtitle A. --Department of Defense

Chapter I. Office of the Secretary of Defense

Subchapter D. Personnel, Military and Civilian

**Part 147.** Adjudicative Guidelines for Determining Eligibility for Access to Classified Information

**Subpart B.** Investigative Standards

**§ 147.18 Introduction.**

The following investigative standards are established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information, to include Sensitive Compartmented Information and Special Access Programs, and are to be used by government departments and agencies as the investigative basis for final clearance determinations. However, nothing in these standards prohibits an agency from using any lawful investigative procedures in addition to these requirements in order to resolve any issue identified in the course of a background investigation or reinvestigation.

SOURCE: [57 FR 6199](#), Feb. 21, 1992; [63 FR 4573](#), Jan. 30, 1998; [68 FR 38609](#), June 30, 2003, unless otherwise noted.

AUTHORITY: [E.O. 12968 \(60 FR 40245; 3 CFR 1995 Comp., p 391\)](#).

32 C. F. R. § 147.18, 32 CFR § 147.18

Current through February 28, 2012; 78 FR 13770

**32 C.F.R. Pt. 147, Subpt. B, Attach. A**

Code of Federal Regulations Currentness Title 32. National Defense Subtitle A. Department of Defense Chapter I. Office of the Secretary of Defense Subchapter D. Personnel, Military and Civilian (Refs & Annos) Part 147. Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (Refs & Annos) Subpart B. Investigative Standards Attachment A to Subpart B of Part 147--Standard A--National Agency Check With Local Agency Checks and Credit Check (NACLC)

...32 C.F.R. Pt. 147, Subpt. B, Attach. A Code of Federal Regulations Currentness Title 32. National Defense Subtitle A . Department of Defense Chapter I . Office of the Secretary of Defense Subchapter D . Personnel, Military and Civilian (Refs & Annos) Part 147 . Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (Refs & Annos) Subpart B . Investigative Standards to Subpart B of Part 147--Standard A--National Agency Check With Local Agency Checks and Credit Check (NACLC) Attachment A to Subpart B of Part 147--Standard A--National Agency Check With Local Agency Checks and Credit Check (NACLC) (a) Applicability. Standard A applies to investigations ...

**32 C.F.R. Pt. 147, Subpt. B, Attach. B**

Code of Federal Regulations Currentness Title 32. National Defense Subtitle A. Department of Defense Chapter I. Office of the Secretary of Defense Subchapter D. Personnel, Military and Civilian (Refs & Annos) Part 147. Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (Refs & Annos) Subpart B. Investigative Standards Attachment B to Subpart B of Part 147--Standard B--Single Scope Background Investigation (SSBI)

...32 C.F.R. Pt. 147, Subpt. B, Attach. B Code of Federal Regulations Currentness Title 32. National Defense Subtitle A. Department of Defense Chapter I. Office of the Secretary of Defense Subchapter D. Personnel, Military and Civilian (Refs & Annos) Part 147. Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (Refs & Annos) Subpart B. Investigative Standards to Subpart B of Part 147--Standard B--Single Scope Background Investigation (SSBI) Attachment B to Subpart B of Part 147--Standard B--Single Scope Background Investigation (SSBI) (a) Applicability. Standard B applies to initial investigations for; (1) Access to TOP ...

**32 C.F.R. Pt. 147, Subpt. B, Attach. C**

Code of Federal Regulations Currentness Title 32. National Defense Subtitle A. Department of Defense Chapter I. Office of the Secretary of Defense Subchapter D. Personnel, Military and Civilian (Refs & Annos) Part 147. Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (Refs & Annos) Subpart B. Investigative Standards Attachment C to Subpart B of Part 147--Standard C--Single Scope Background Investigation Periodic Reinvestigation (SSBI-PR)

...32 C.F.R. Pt. 147, Subpt. B, Attach. C Code of Federal Regulations Currentness Title 32. National Defense Subtitle A. Department of Defense Chapter I. Office of the Secretary of Defense Subchapter D. Personnel, Military and Civilian (Refs & Annos) Part 147. Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (Refs & Annos) Subpart B. Investigative Standards to Subpart B of Part 147--Standard C--Single Scope Background Investigation Periodic Reinvestigation (SSBI-PR) Attachment C to Subpart B of Part 147--Standard C--Single Scope Background Investigation Periodic Reinvestigation (SSBI-PR) (a) Applicability. Standard C applies to reinvestigation for; (1) Access ...

**32 C.F.R. Pt. 147, Subpt. B, Attach. D**

Code of Federal Regulations Currentness Title 32. National Defense Subtitle A. Department of Defense Chapter I. Office of the Secretary of Defense Subchapter D. Personnel, Military and Civilian (Refs & Annos) Part 147. Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (Refs & Annos) Subpart B. Investigative Standards Attachment D to Subpart B of Part 147--Standard D--Decision Tables

...32 C.F.R. Pt. 147, Subpt. B, Attach. D Code of Federal Regulations Currentness Title 32. National Defense Subtitle A. Department of Defense Chapter I. Office of the Secretary of Defense Subchapter D. Personnel, Military and Civilian (Refs & Annos) Part 147. Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (Refs & Annos) Subpart B. Investigative Standards to Subpart B of Part 147--Standard D--Decision Tables Attachment D to Subpart B of Part 147--Standard D--Decision Tables TABLE 1.-- WHICH INVESTIGATION TO REQUEST If the requirement is for And the person has this ...

•**Title 32, CFR, Part 2001 - Classified National Security Information**

- This is the implementing directive (final rule) issued pursuant to *Executive Order 13526* relating to classified national security information.

**§ 2001.1 Purpose and scope.**

(a) This part is issued under [Executive Order. \(E.O.\) 13526](#), Classified National Security Information (the Order). Section 5 of the Order provides that the Director of the Information Security Oversight Office (ISOO) shall develop and issue such directives as are necessary to implement the Order.

(b) The Order provides that these directives are binding on agencies. Section 6.1(a) of the Order defines “agency” to mean any “Executive agency” as defined in [5 U.S.C. 105](#); any “Military department” as defined in [5 U.S.C. 102](#); and any other entity within the executive branch that comes into the possession of classified information.

(c) For the convenience of the user, the following table provides references between the sections contained in this part and the relevant sections of the Order.

CFR section		Related section of E.O. 13526
2001.10	Classification standards	1.1, 1.4
2001.11	Original classification authority	1.3
2001.12	Duration of classification	1.5
2001.13	Classification prohibitions and limitations	1.7
2001.14	Classification challenges	1.8
2001.15	Classification guides	2.2
2001.16	Fundamental classification guidance review	1.9
2001.20	General	1.6
2001.21	Original classification	1.6(a)
2001.22	Derivative classification	2.1
2001.23	Classification marking in the electronic environment	1.6
2001.24	Additional	1.6

	requirements	
2001.25	Declassification markings	1.5, 1.6, 3.3
2001.26	Automatic declassification exemption markings	3.3
2001.30	Automatic declassification	3.3, 3.7
2001.31	Systematic declassification review	3.4
2001.32	Declassification guides	3.3, 3.7
2001.33	Mandatory review for declassification	3.5, 3.6
2001.34	Referrals	3.3, 3.6, 3.7
2001.35	Discretionary declassification	3.1
2001.36	Classified information in the custody of private organizations or individuals	none
2001.37	Assistance to the Department of State	none
2001.40	General	4.1
2001.41	Responsibilities of holders	4.1
2001.42	Standards for security equipment	4.1
2001.43	Storage	4.1
2001.44	Reciprocity of use and inspection of facilities	4.1
2001.45	Information controls	4.1, 4.2
2001.46	Transmission	4.1, 4.2
2001.47	Destruction	4.1, 4.2
2001.48	Loss, possible compromise, or unauthorized disclosure	4.1, 4.2
2001.49	Special access programs	4.3
2001.50	Telecommunications, automated information systems, and network security	4.1, 4.2
2001.51	Technical security	4.1
2001.52	Emergency authority	4.2
2001.53	Open storage areas	4.1



2001.54	Foreign government information	4.1
2001.55	Foreign disclosure of classified information	4.1(i)(2)
2001.60	Self-Inspections, General	5.4
2001.70	Security Education and Training, General	5.4
2001.71	Coverage	1.3(d), 2.1(d), 3.7(b), 4.1(b), 5.4(d)(3)
2001.80	Prescribed standard forms	5.2(b)(7)
2001.90	Agency annual reporting requirements	1.3(c), 5.2(b)(4), 5.4(d)(4), 5.4(d)(8)
2001.91	Other agency reporting requirements	1.3(d), 1.7(c)(3), 1.9(d), 2.1(d), 5.5
2001.92	Definitions	6.1

<Part amended by [75 FR 37254](#), retroactively effective June 25, 2010.>

SOURCE: [75 FR 37254](#), June 28, 2010, unless otherwise noted.

**AUTHORITY:** [Sections 5.1\(a\) and \(b\), E.O. 13526, \(75 FR 707, January 5, 2010\).](#)

32 C. F. R. § 2001.1, 32 CFR § 2001.1

Current through February 28, 2012; 78 FR 13770

**•Title 41, CFR, Part 102-74 – Facility Management, Subpart C - Conduct on Federal Property**

**§ 102-74.365 To whom does this subpart apply?**

The rules in this subpart apply to all property under the authority of GSA and to all persons entering in or on such property. Each occupant agency shall be responsible for the observance of these rules and regulations. Federal agencies must post the notice in the Appendix to this part at each public entrance to each Federal facility.

**§ 102-74.370 What items are subject to inspection by Federal agencies?**

Federal agencies may, at their discretion, inspect packages, briefcases and other containers in the immediate possession of visitors, employees or other persons arriving on, working at, visiting, or departing from Federal property. Federal agencies may conduct a full search of a person and the vehicle the person is driving or occupying upon his or her arrest.

## **Executive Orders**

### **•EO 13587 - Structural Reforms to Improve the Security of Classified Networks and Responsible Sharing and Safeguarding of Classified Information**

Section 1. Policy. Our Nation's security requires classified information to be shared immediately with authorized users around the world but also requires sophisticated and vigilant means to ensure it is shared securely. Computer networks have individual and common vulnerabilities that require coordinated decisions on risk management.

This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), and all classified information on those networks.

#### Sec. 2. General Responsibilities of Agencies.

Sec. 2.1. The heads of agencies that operate or access classified computer networks shall have responsibility for appropriately sharing and safeguarding classified information on computer networks. As part of this responsibility, they shall:

- (a) designate a senior official to be charged with overseeing classified information sharing and safeguarding efforts for the agency;
- (b) implement an insider threat detection and prevention program consistent with guidance and standards developed by the Insider Threat Task Force established in section 6 of this order;
- (c) perform self-assessments of compliance with policies and standards issued pursuant to sections 3.3, 5.2, and 6.3 of this order, as well as other applicable policies and standards, the results of which shall be reported annually to the Senior Information Sharing and Safeguarding Steering Committee established in section 3 of this order;
- (d) provide information and access, as warranted and consistent with law and section 7(d) of this order, to enable independent assessments by the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force of compliance with relevant established policies and standards; and
- (e) detail or assign staff as appropriate and necessary to the Classified Information Sharing and Safeguarding Office and the Insider Threat Task Force on an ongoing basis.

#### Sec. 6. Insider Threat Task Force.

Sec. 6.1. There is established an interagency Insider Threat Task Force that shall develop a Government-

wide program (insider threat program) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies. This program shall include development of policies, objectives, and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices within agencies.

Sec. 6.2. The Task Force shall be co-chaired by the Attorney General and the Director of National Intelligence, or their designees. Membership on the Task Force shall be composed of officers of the United States from, and designated by the heads of, the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the ISOO, as well as such additional agencies as the co-chairs of the Task Force may designate. It shall be staffed by personnel from the Federal Bureau of Investigation and the Office of the National Counterintelligence Executive (ONCIX), and other agencies, as determined by the co-chairs for their respective agencies and to the extent permitted by law. Such personnel must be officers or full-time or permanent part-time employees of the United States. To the extent permitted by law, ONCIX shall provide an appropriate work site and administrative support for the Task Force.

Sec. 6.3. The Task Force's responsibilities shall include the following:

- (a) developing, in coordination with the Executive Agent, a Government-wide policy for the deterrence, detection, and mitigation of insider threats, which shall be submitted to the Steering Committee for appropriate review;
- (b) in coordination with appropriate agencies, developing minimum standards and guidance for implementation of the insider threat program's Government-wide policy and, within 1 year of the date of this order, issuing those minimum standards and guidance, which shall be binding on the executive branch;
- (c) if sufficient appropriations or authorizations are obtained, continuing in coordination with appropriate agencies after 1 year from the date of this order to add to or modify those minimum standards and guidance, as appropriate;
- (d) if sufficient appropriations or authorizations are not obtained, recommending for promulgation by the Office of Management and Budget or the ISOO any additional or modified minimum standards and guidance developed more than 1 year after the date of this order;
- (e) referring to the Steering Committee for resolution any unresolved issues delaying the timely development and issuance of minimum standards;
- (f) conducting, in accordance with procedures to be developed by the Task Force, independent assessments of the adequacy of agency programs to implement established policies and minimum standards, and reporting the results of such assessments to the Steering Committee;
- (g) providing assistance to agencies, as requested, including through the dissemination of best practices; and
- (h) providing analysis of new and continuing insider threat challenges facing the United States Government.

**\*Writer's note: See also Presidential Memorandum for the Heads of Executive Departments and Agencies, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," dated November 21, 2012.**

**•EO 13549 - Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities**

By the authority vested in me as President by the Constitution and the laws of the United States of America, in order to ensure the proper safeguarding of information shared with State, local, tribal, and private sector entities, it is hereby ordered as follows:

Section 1. Establishment and Policy.

Sec. 1.1. There is established a Classified National Security Information Program (Program) designed to safeguard and govern access to classified national security information shared by the Federal Government with State, local, tribal, and private sector (SLTPS) entities.

Sec. 1.2. The purpose of this order is to ensure that security standards governing access to and safeguarding of classified material are applied in accordance with [Executive Order 13526](#) of December 29, 2009 ("Classified National Security Information"), [Executive Order 12968](#) of August 2, 1995, as amended ("Access to Classified Information"), [Executive Order 13467](#) of June 30, 2008 ("Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information"), and [Executive Order 12829](#) of January 6, 1993, as amended ("National Industrial Security Program"). Procedures for uniform implementation of these standards by SLTPS entities shall be set forth in an implementing directive to be issued by the Secretary of Homeland Security within 180 days of the date of this order, in consultation with affected executive departments and agencies (agencies), and with the concurrence of the Secretary of Defense, the Attorney General, the Director of National Intelligence, and the Director of the Information Security Oversight Office.

Sec. 1.3. Additional policy provisions for access to and safeguarding of classified information shared with SLTPS personnel include the following:

- (a) Eligibility for access to classified information by SLTPS personnel shall be determined by a sponsoring agency. The level of access granted shall not exceed the Secret level, unless the sponsoring agency determines on a case-by-case basis that the applicant has a demonstrated and foreseeable need for access to Top Secret, Special Access Program, or Sensitive Compartmented Information.
- (b) Upon the execution of a non-disclosure agreement prescribed by the Information Security Oversight Office or the Director of National Intelligence, and absent disqualifying conduct as determined by the clearance granting official, a duly elected or appointed Governor of a State or territory, or an official who has succeeded to that office under applicable law, may be granted access to classified information without a background investigation in accordance with the implementing directive for this order. This authorization of access may not be further delegated by the Governor to any other person.
- (c) All clearances granted to SLTPS personnel, as well as accreditations granted to SLTPS facilities without a waiver, shall be accepted reciprocally by all agencies and SLTPS entities.
- (d) Physical custody of classified information by State, local, and tribal (SLT) entities shall be limited to

Secret information unless the location y51610housing the information is under the full-time management, control, and operation of the Department of Homeland Security or another agency. A standard security agreement, established by the Department of Homeland Security in consultation with the SLTPS Advisory Committee, shall be executed between the head of the SLT entity and the U.S. Government for those locations where the SLT entity will maintain physical custody of classified information.

(e) State, local, and tribal facilities where classified information is or will be used or stored shall be inspected, accredited, and monitored for compliance with established standards, in accordance with [Executive Order 13526](#) and the implementing directive for this order, by the Department of Homeland Security or another agency that has entered into an agreement with the Department of Homeland Security to perform such inspection, accreditation, and monitoring.

(f) Private sector facilities where classified information is or will be used or stored shall be inspected, accredited, and monitored for compliance with standards established pursuant to [Executive Order 12829](#), as amended, by the Department of Defense or the cognizant security agency under [Executive Order 12829](#), as amended.

(g) Access to information systems that store, process, or transmit classified information shall be enforced by the rules established by the agency that controls the system and consistent with approved dissemination and handling markings applied by originators, separate from and in addition to criteria for determining eligibility for access to classified information. Access to information within restricted portals shall be based on criteria applied by the agency that controls the portal and consistent with approved dissemination and handling markings applied by originators.

(h) The [National Industrial Security Program established in Executive Order 12829](#), as amended, shall govern the access to and safeguarding of classified information that is released to contractors, licensees, and grantees of SLT entities.

(i) All access eligibility determinations and facility security accreditations granted prior to the date of this order that do not meet the standards set forth in this order or its implementing directive shall be reconciled with those standards within a reasonable period.

(j) Pursuant to section 4.1(i)(3) of [Executive Order 13526](#), documents created prior to the effective date of [Executive Order 13526](#) shall not be re-disseminated to other entities without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information that originated within that agency.

Sec. 2. Policy Direction. With policy guidance from the National Security Advisor and in consultation with the Director of the Information Security Oversight Office, the Director of the Office of Management and Budget, and the heads of affected agencies, the Secretary of Homeland Security shall serve as the Executive Agent for the Program. This order does not displace any authorities provided by law or Executive Order and the Executive Agent shall, to the extent practicable, make use of existing structures and authorities to preclude duplication and to ensure efficiency.

Sec. 4. Operations and Oversight. (a) The Executive Agent for the Program shall perform the following responsibilities:

(1) overall program management and oversight;

(2) accreditation, periodic inspection, and monitoring of all facilities owned or operated by SLT entities that have access to classified information, except when another agency has entered into an agreement with the Department of Homeland Security to perform some or all of these functions;

(3) processing of security clearance applications by SLTPS personnel, when requested by a sponsoring agency, on a reimbursable basis unless otherwise determined by the Department of Homeland Security and the sponsoring agency;

(4) documenting and tracking the final status of security clearances for all SLTPS personnel in consultation with the Office of Personnel Management, the Department of Defense, and the Office of the Director of National Intelligence;

(5) developing and maintaining a security profile of SLT facilities that have access to classified information; and

(6) developing training, in consultation with the Committee, for all SLTPS personnel who have been determined eligible for access to classified information, which shall cover the proper safeguarding of classified information and sanctions for unauthorized disclosure of classified information.

(b) The Secretary of Defense, or the cognizant security agency under Executive Order 12829, as amended, shall provide program management, oversight, inspection, accreditation, and monitoring of all private sector facilities that have access to classified information.

(c) The Director of National Intelligence may inspect and monitor SLTPS programs and facilities that involve access to information regarding intelligence sources, methods, and activities.

(d) Heads of agencies that sponsor SLTPS personnel and facilities for access to and storage of classified information under section 1.3(a) of this order shall:

(1) ensure on a periodic basis that there is a demonstrated, foreseeable need for such access; and

(2) provide the Secretary of Homeland Security with information, as requested by the Secretary, about SLTPS personnel sponsored for security clearances and SLT facilities approved for use of classified information prior to and after the date of this order, except when the disclosure of the association of a

specific individual with an intelligence or law enforcement agency must be protected in the interest of national security, as determined by the intelligence or law enforcement agency.

Sec. 5. Definitions. For purposes of this order:

(a) “Access” means the ability or opportunity to gain knowledge of classified information.

(b) “Agency” means any “Executive agency” as defined in [5 U.S.C. 105](#); any military department as defined in [5 U.S.C. 102](#); and any other entity within the executive branch that comes into possession of classified information.

(c) “Classified National Security Information” or “classified information” means information that has been determined pursuant to Executive Order [13526](#), or any predecessor or successor order, to require protection against unauthorized disclosure, and is marked to indicate its classified status when in documentary form.

(d) “Information” means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government.

(e) “Intelligence activities” means all activities that elements of the Intelligence Community are authorized to conduct pursuant to law or [Executive Order 12333](#), as amended, or a successor order.

(f) “Local” entities refers to “(A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; and (B) a rural community, unincorporated town or village, or other public entity” as defined in section 2 of the Homeland Security Act of 2002 ([6 U.S.C. 101\(11\)](#)).

(g) “Private sector” means persons outside government who are critically involved in ensuring that public and private preparedness and response efforts are integrated as part of the Nation's Critical Infrastructure or Key Resources (CIKR), including:

(1) corporate owners and operators determined by the Secretary of Homeland Security to be part of the CIKR;

(2) subject matter experts selected to assist the Federal or State CIKR;

(3) personnel serving in specific leadership positions of CIKR coordination, operations, and oversight;

(4) employees of corporate entities relating to the protection of CIKR; or

(5) other persons not otherwise eligible for the granting of a personnel security clearance pursuant to [Executive Order 12829](#), as amended, who are determined by the Secretary of Homeland Security to require a personnel security clearance.

(h) “Restricted portal” means a protected community of interest or similar area housed within an information system and to which access is controlled by a host agency different from the agency that controls the information system.

(i) “Sponsoring Agency” means an agency that recommends access to or possession of classified information by SLTPS personnel.

(j) “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States, as defined in section 2 of the Homeland Security Act of 2002 ([6 U.S.C. 101\(15\)](#)).

(k) “State, local, and tribal personnel” means any of the following persons:

(1) Governors, mayors, tribal leaders, and other elected or appointed officials of a State, local government, or tribe;

(2) State, local, and tribal law enforcement personnel and firefighters;

(3) public health, radiological health, and medical professionals of a State, local government, or tribe; and



(4) regional, State, local, and tribal emergency management agency personnel, including State Adjutants General and other appropriate public safety personnel and those personnel providing support to a Federal CIKR mission.

(l) “Tribe” means any Indian or Alaska Native tribe, band, nation, pueblo, village, or community that the Secretary of the Interior acknowledges to exist as an Indian tribe as defined in the Federally Recognized Tribe List Act of 1994 ([25 U.S.C. 479a\(2\)](#)).

(m) “United States” when used in a geographic sense, means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, any possession of the United States and any waters within the territorial jurisdiction of the United States.

Sec. 6. General Provisions. (a) This order does not change the requirements of [Executive Orders 13526, 12968, 13467](#), or 12829, as amended, and their successor orders and directives.

(b) Nothing in this order shall be construed to supersede or change the authorities of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended ([42 U.S.C. 2011 et seq.](#)); the Secretary of Defense under [Executive Order 12829](#), as amended; the Director of the [Information Security Oversight Office under Executive Order 13526](#) and [Executive Order 12829](#), as amended; the Attorney General under title 18, United States Code, and the Foreign Intelligence Surveillance Act ([50 U.S.C. 1801 et seq.](#)); the Secretary of State under title 22, United States Code, and the Omnibus Diplomatic Security and Antiterrorism Act of 1986; or the Director of National Intelligence under the National Security Act of 1947, as amended, [Executive Order 12333](#), as amended, [Executive Order 12968](#), as amended, [Executive Order 13467](#), and [Executive Order 13526](#).

(c) Nothing in this order shall limit the authority of an agency head, or the agency head's designee, to authorize in an emergency and when necessary to respond to an imminent threat to life or in defense of the homeland, in accordance with section 4.2(b) of [Executive Order 13526](#), the disclosure of classified information to an individual or individuals who are otherwise not eligible for access in accordance with the provisions of [Executive Order 12968](#).

(d) Consistent with section 892(a)(4) of the Homeland Security Act of 2002 ([6 U.S.C. 482\(a\)\(4\)](#)), nothing in this order shall be interpreted as changing the requirements and authorities to protect sources and methods.

(e) Nothing in this order shall supersede measures established under the authority of law or Executive Order to protect the security and integrity of specific activities and associations that are in direct support of intelligence operations.

(f) Pursuant to section 892(e) of the Homeland Security Act of 2002 ([6 U.S.C. 482\(e\)](#)), all information provided to an SLTPS entity from an agency shall remain under the control of the Federal Government. Any State or local law authorizing or requiring disclosure shall not apply to such information.

(g) Nothing in this order limits the protection afforded any classified information by other provisions of law. This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(h) Nothing in this order shall be construed to obligate action or otherwise affect functions by the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(i) This order shall be implemented subject to the availability of appropriations and consistent with procedures approved by the Attorney General pursuant to [Executive Order 12333](#), as amended.

**•EO 13526 - Classified National Security Information**

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information both within the Government and to the American people. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.

PART 4 -- SAFEGUARDING

Sec. 4.1. General Restrictions on Access. (a) A person may have access to classified information provided that:

(1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;

(2) the person has signed an approved nondisclosure agreement; and

(3) the person has a need-to-know the information.

(b) Every person who has met the standards for access to classified information in paragraph (a) of this section shall receive contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

(c) An official or employee leaving agency service may not remove classified information from the agency's control or direct that information be declassified in order to remove it from agency control.

(d) Classified information may not be removed from official premises without proper authorization.

(e) Persons authorized to disseminate classified information outside the executive branch shall ensure the protection of the information in a manner equivalent to that provided within the executive branch.

(f) Consistent with law, executive orders, directives, and regulations, an agency head or senior agency official or, with respect to the Intelligence Community, the Director of National Intelligence, shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information:

(1) prevent access by unauthorized persons;

(2) ensure the integrity of the information; and

(3) to the maximum extent practicable, use:

(A) common information technology standards, protocols, and interfaces that maximize the availability of, and access to, the information in a form and manner that facilitates its authorized use; and

(B) standardized electronic formats to maximize the accessibility of information to persons who meet the criteria set forth in section 4.1(a) of this order.

(g) Consistent with law, executive orders, directives, and regulations, each agency head or senior agency official, or with respect to the Intelligence Community, the Director of National Intelligence, shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

Sec. 4.3. Special Access Programs. (a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence sources, methods, and activities (but not including military operational, strategic, and tactical programs), this function shall be exercised by the Director of National Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only when the program is required by statute or upon a specific finding that:

(1) the vulnerability of, or threat to, specific information is exceptional; and

(2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.

(b) Requirements and limitations. (1) Special access programs shall be limited to programs in which the number of persons who ordinarily will have access will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.

Sec. 5.4. General Responsibilities. Heads of agencies that originate or handle classified information shall:

(a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order;

(b) commit necessary resources to the effective implementation of the program established under this order;

(c) ensure that agency records systems are designed and maintained to optimize the appropriate sharing and safeguarding of classified information, and to facilitate its declassification under the terms of this order when it no longer meets the standards for continued classification; and

(d) designate a senior agency official to direct and administer the program, whose responsibilities shall include:

(1) overseeing the agency's program established under this order, provided an agency head may designate a separate official to oversee special access programs authorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;

(2) promulgating implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public;

(3) establishing and maintaining security education and training programs;

(4) establishing and maintaining an ongoing self-inspection program, which shall include the regular reviews of representative samples of the agency's original and derivative classification actions, and shall authorize appropriate agency officials to correct misclassification actions not covered by sections 1.7(c) and 1.7(d) of this order; and reporting annually to the Director of the Information Security Oversight Office on the agency's self-inspection program;

(5) establishing procedures consistent with directives issued pursuant to this order to prevent unnecessary access to classified information, including procedures that:

(A) require that a need for access to classified information be established before initiating administrative clearance procedures; and

(B) ensure that the number of persons granted access to classified information meets the mission needs of the agency while also satisfying operational and security requirements and needs;

(6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(7) ensuring that the performance contract or other system used to rate civilian or military personnel performance includes the designation and management of classified information as a critical element or item to be evaluated in the rating of:

(A) original classification authorities;

(B) security managers or security specialists; and

(C) all other personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings;

(8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication;

(9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function; and

(10) establishing a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the agency and to provide guidance to personnel on proper

classification as needed.

**•EO 13488 - Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust**

By the authority vested in me as President by the Constitution and the laws of the United States of America, including sections 1104(a)(1), 3301, and 7301 of title 5, United States Code, and in order to simplify and streamline the system of Federal Government personnel investigative and adjudicative processes to make them more efficient and effective, it is hereby ordered as follows:

Section 1. Policy. (a) When agencies determine the fitness of individuals to perform work as employees in the excepted service or as contractor employees, prior favorable fitness or suitability determinations should be granted reciprocal recognition, to the extent practicable.

(b) It is necessary to reinvestigate individuals in positions of public trust in order to ensure that they remain suitable for continued employment.

Sec. 2. Definitions. For the purposes of this order:

(a) “Agency” means an executive agency as defined in section 105 of title 5, United States Code, but does not include the Government Accountability Office.

(b) “Contractor employee” means an individual who performs work for or on behalf of any agency under a contract and who, in order to perform the work specified under the contract, will require access to space, information, information technology systems, staff, or other assets of the Federal Government. Such contracts, include, but are not limited to:

(i) personal services contracts;

(ii) contracts between any non-Federal entity and any agency; and

(iii) sub-contracts between any non-Federal entity and another non-Federal entity to perform work related to the primary contract with the agency.

(c) “Excepted service” has the meaning provided in section 2103 of title 5, United States Code, but does not include those positions in any element of the intelligence community as defined in the National Security Act of 1947, as amended, to the extent they are not otherwise subject to Office of Personnel Management appointing authorities.

(d) “Fitness” is the level of character and conduct determined necessary for an individual to perform work for or on behalf of a Federal agency as an employee in the excepted service (other than a position subject to suitability) or as a contractor employee.

(e) “Fitness determination” means a decision by an agency that an individual has or does not have the required level of character and conduct necessary to perform work for or on behalf of a Federal agency as an employee in the excepted service (other than a position subject to suitability) or as a contractor employee. A favorable fitness determination is not a decision to appoint or contract with an individual.

(f) “Position of Public Trust” has the meaning provided in 5 CFR Part 731.

(g) "Suitability" has the meaning and coverage provided in CFR Part 731.

Sec. 3. Agency Authority to Set Fitness Criteria and Determine Equivalency. The authority to establish criteria for making fitness determinations remains within the discretion of the agency head. Agency heads also have the discretion to determine whether their criteria are equivalent to suitability standards established by the Office of Personnel Management. Agency heads shall take into account Office of Personnel Management guidance when exercising this discretion.

Sec. 4. Reciprocal Recognition of Fitness and Suitability Determinations.(a) Except as provided by subsection (b) of this section, agencies making fitness determinations shall grant reciprocal recognition to a prior favorable fitness or suitability determination when:

(i) the gaining agency uses criteria for making fitness determinations equivalent to suitability standards established by the Office of Personnel Management;

(ii) the prior favorable fitness or suitability determination was based on criteria equivalent to suitability standards established by the Office of Personnel Management; and

(iii) the individual has had no break in employment since the favorable determination was made.

(b) Exceptions to Reciprocal Recognition. A gaining agency is not required to grant reciprocal recognition to a prior favorable fitness or suitability determination when:

(i) the new position requires a higher level of investigation than previously conducted for that individual;

(ii) an agency obtains new information that calls into question the individual's fitness based on character or conduct; or

(iii) the individual's investigative record shows conduct that is incompatible with the core duties of the new position.

Sec. 5. Reinvestigation of Individuals in Positions of Public Trust. Individuals in positions of public trust shall be subject to reinvestigation under standards (including but not limited to the frequency of such reinvestigation) as determined by the Director of the Office of Personnel Management, to ensure their suitability for continued employment.

Sec. 6. Responsibilities.(a) An agency shall report to the Office of Personnel Management the nature and results of the background investigation and fitness determination (or later changes to that determination) made on an individual, to the extent consistent with law.

(b) The Director of the Office of Personnel Management is delegated authority to implement this order, including the authority to issue regulations and guidance governing suitability, or guidance related to fitness, as the Director determines appropriate.

Sec. 7. General Provisions.(a) Nothing in this order shall be construed to impair or otherwise affect:

(i) authority granted by law to a department or agency, or the head thereof; or

(ii) functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order shall not suspend, impede, or otherwise affect Executive Order 10450 of April 27, 1953, as amended, or Executive Order 13467 of June 30, 2008;

(d) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its agencies, instrumentalities, or entities, its officers, employees or agents, or any other person.

Sec. 8. Effective Date and Applicability. This order is effective upon issuance and is applicable to individuals newly appointed to excepted service positions or hired as contractor employees beginning 90 days from the effective date of this order.

**•EO 13467 - Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information**

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to ensure an efficient, practical, reciprocal, and aligned system for investigating and determining suitability for Government employment, contractor employee fitness, and eligibility for access to classified information, while taking appropriate account of title III of Public Law 108-458, it is hereby ordered as follows:

**PART 1 - POLICY, APPLICABILITY, AND DEFINITIONS**

Section 1.1. Policy. Executive branch policies and procedures relating to suitability, contractor employee fitness, eligibility to hold a sensitive position, access to federally controlled facilities and information systems, and eligibility for access to classified information shall be aligned using consistent standards to the extent possible, provide for reciprocal recognition, and shall ensure cost-effective, timely, and efficient protection of the national interest, while providing fair treatment to those upon whom the Federal Government relies to conduct our Nation's business and protect national security.

Sec. 1.2. Applicability. (a) This order applies to all covered individuals as defined in section 1.3(g), except that:

(i) the provisions regarding eligibility for physical access to federally controlled facilities and logical access to federally controlled information systems do not apply to individuals exempted in accordance with guidance pursuant to the Federal Information Security Management Act (title III of Public Law 107-347) and Homeland Security Presidential Directive 12; and

(ii) the qualification standards for enlistment, appointment, and induction into the Armed Forces pursuant to title 10, United States Code, are unaffected by this order.

(b) This order also applies to investigations and determinations of eligibility for access to classified information for employees of agencies working in or for the legislative or judicial branches when those investigations or determinations are conducted by the executive branch.

Sec. 1.3. Definitions. For the purpose of this order:

(a) “Adjudication” means the evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is:

- (i) suitable for Government employment;
- (ii) eligible for logical and physical access;
- (iii) eligible for access to classified information;
- (iv) eligible to hold a sensitive position; or
- (v) fit to perform work for or on behalf of the Government as a contractor employee.

(b) “Agency” means any “Executive agency” as defined in section 105 of title 5, United States Code, including the “military departments,” as defined in section 102 of title 5, United States Code, and any other entity [within the executive branch that comes into possession of classified information or has designated positions as sensitive, except such an entity headed by an officer who is not a covered individual.

(c) “Classified information” means information that has been determined pursuant to Executive Order 12958 of April 17, 1995, as amended, or a successor or predecessor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011et seq.) to require protection against unauthorized disclosure.

(d) “Continuous evaluation” means reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information.

(e) “Contractor” means an expert or consultant (not appointed under section 3109 of title 5, United States Code) to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of any agency, including all subcontractors; a personal services contractor; or any other category of person who performs work for or on behalf of an agency (but not a Federal employee).

(f) “Contractor employee fitness” means fitness based on character and conduct for work for or on behalf of the Government as a contractor employee.

(g) “Covered individual” means a person who performs work for or on behalf of the executive branch, or who seeks to perform work for or on behalf of the executive branch, but does not include:

- (i) the President or (except to the extent otherwise directed by the President) employees of the President under section 105 or 107 of title 3, United States Code; or

- (ii) the Vice President or (except to the extent otherwise directed by the Vice President) employees of the Vice President under section 106 of title 3 or annual legislative branch appropriations acts.

(h) “End-to-end automation” means an executive branch-wide federated system that uses automation to manage and monitor cases and maintain relevant documentation of the application (but not



an employment application), investigation, adjudication, and continuous evaluation processes.

(i) “Federally controlled facilities” and “federally controlled information systems” have the meanings prescribed in guidance pursuant to the Federal Information Security Management Act (title III of Public Law 107-347) and Homeland Security Presidential Directive 12.

(j) “Logical and physical access” means access other than occasional or intermittent access to federally controlled facilities or information systems.

(k) “Sensitive position” means any position so designated under Executive Order 10450 of April 27, 1953, as amended.

(l) “Suitability” has the meaning and coverage provided in 5 CFR Part 731.

## PART 2 - ALIGNMENT, RECIPROCITY, AND GOVERNANCE

Sec. 2.1. Aligned System.(a) Investigations and adjudications of covered individuals who require a determination of suitability, eligibility for logical and physical access, eligibility to hold a sensitive position, eligibility for access to classified information, and, as appropriate, contractor employee fitness, shall be aligned using consistent standards to the extent possible. Each successively higher level of investigation and adjudication shall build upon, but not duplicate, the ones below it.

(b) The aligned system shall employ updated and consistent standards and methods, enable innovations with enterprise information technology capabilities and end-to-end automation to the extent practicable, and ensure that relevant information maintained by agencies can be accessed and shared 38105[rapidly across the executive branch, while protecting national security, protecting privacy-related information, ensuring resulting decisions are in the national interest, and providing the Federal Government with an effective workforce.

(c) Except as otherwise authorized by law, background investigations and adjudications shall be mutually and reciprocally accepted by all agencies. An agency may not establish additional investigative or adjudicative requirements (other than requirements for the conduct of a polygraph examination consistent with law, directive, or regulation) that exceed the requirements for suitability, contractor employee fitness, eligibility for logical or physical access, eligibility to hold a sensitive position, or eligibility for access to classified information without the approval of the Suitability Executive Agent or Security Executive Agent, as appropriate, and provided that approval to establish additional requirements shall be limited to circumstances where additional requirements are necessary to address significant needs unique to the agency involved or to protect national security.

Sec. 2.4. Additional Functions. (a) The duties assigned to the Security Policy Board by Executive Order 12968 of August 2, 1995, to consider, coordinate, and recommend policy directives for executive branch security policies, procedures, and practices are reassigned to the Security Executive Agent.

### (b) Heads of agencies shall:

(i) carry out any function assigned to the agency head by the Chair, and shall assist the Chair, the Council, the Suitability Executive Agent, and the Security Executive Agent in carrying out any function under sections 2.2 and 2.3 of this order;

(ii) implement any policy or procedure developed pursuant to this order;

(iii) to the extent permitted by law, make available to the Performance Accountability Council, the Suitability Executive Agent, or the Security 38107 [Executive Agent such information as may be requested to implement this order;

(iv) ensure that all actions taken under this order take account of the counterintelligence interests of the United States, as appropriate; and

(v) ensure that actions taken under this order are consistent with the President's constitutional authority to:

(A) conduct the foreign affairs of the United States;

(B) withhold information the disclosure of which could impair the foreign relations, the national security, the deliberative processes of the Executive, or the performance of the Executive's constitutional duties;

(C) recommend for congressional consideration such measures as the President may judge necessary or expedient; and

(D) supervise the unitary executive branch.

### Sec. 3. General Provisions.

Executive Order 12968 of August 2, 1995 is amended:

(i) by inserting: "Sec. 3.5. Continuous Evaluation. An individual who has been determined to be eligible for or who currently has access to classified information shall be subject to continuous evaluation under standards (including, but not limited to, the frequency of such evaluation) as determined by the Director of National Intelligence."

### **•EO 13286 - Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security**

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the Homeland Security Act of 2002 ([Public Law 107-296](#)) and [section 301 of title 3, United States Code](#), and in order to reflect the transfer of certain functions to, and other responsibilities vested in, the Secretary of Homeland Security, the transfer of certain agencies and agency components to the Department of Homeland Security, and the delegation of appropriate responsibilities to the Secretary of Homeland Security, it is hereby ordered as follows:

The heads of executive branch departments and agencies are responsible and accountable for providing and maintaining adequate levels of security for information systems, including emergency preparedness communications systems, for programs under their control. Heads of such departments and agencies shall ensure the development and, within available appropriations, funding of programs that adequately address these mission systems, especially those critical systems that support the national security and other essential government programs.

•**EO 13231 - Critical Infrastructure Protection in the Information Age**

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to ensure protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, in the information age, it is hereby ordered as follows:

**Section 1. Policy.**

(a) The information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. Those three functions now depend on an interdependent network of critical information infrastructures. The protection program authorized by this order shall consist of continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. Protection of these systems is essential to the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services sectors.

(b) It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. The implementation of this policy shall include a voluntary public-private partnership, involving corporate and nongovernmental organizations.

**Sec. 2. Scope.** To achieve this policy, there shall be a senior executive branch board to coordinate and have cognizance of Federal efforts and programs that relate to protection of information systems and involve:

(a) cooperation with and protection of private sector critical infrastructure, State and local governments' critical infrastructure, and supporting programs in corporate and academic organizations;

(b) protection of Federal departments' and agencies' critical infrastructure; and

(c) related national security programs.

**Sec. 4. Continuing Authorities**

***Additional Responsibilities: The Heads of Executive Branch Departments and Agencies.*** The heads of executive branch departments and agencies are responsible and accountable for providing and maintaining adequate levels of security for information systems, including emergency preparedness communications systems, for programs under their control. Heads of such departments and agencies shall ensure the development and, within available appropriations, funding of programs that adequately address these mission areas. Cost-effective security shall be built into and made an integral part of government information systems, especially those critical systems that support the national security and other essential government programs. Additionally, security should enable, and not unnecessarily impede, department and agency business operations.

•**EO 12968 - Access to Classified Information**

The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life.

Security policies designed to protect classified information must ensure consistent, cost effective, and efficient protection of our Nation's classified information, while providing fair and equitable treatment to those Americans upon whom we rely to guard our national security.

This order establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information.

**PART 1—DEFINITIONS, ACCESS TO CLASSIFIED INFORMATION, FINANCIAL DISCLOSURE, AND OTHER ITEMS**

**Section 1.1. Definitions.** For the purposes of this order: (a) “Agency” means any “Executive agency,” as defined in 5 U.S.C. 105, the “military departments,” as defined in 5 U.S.C. 102, and any other entity within the executive branch that comes into the possession of classified information, including the Defense Intelligence Agency, National Security Agency, and the National Reconnaissance Office.

(b) “Applicant” means a person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information.

(c) “Authorized investigative agency” means an agency authorized by law or regulation to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.

(d) “Classified information” means information that has been determined pursuant to Executive Order No. 12958, or any successor order, Executive Order No. 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure.

(e) “Employee” means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

(f) “Foreign power” and “agent of a foreign power” have the meaning provided in 50 U.S.C. 1801.

(g) “Need for access” means a determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized governmental function.

(h) “Need-to-know” means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(i) “Overseas Security Policy Board” means the Board established by the President to consider, develop, coordinate and promote policies, standards and agreements on overseas security operations, programs and

projects that affect all United States Government agencies under the authority of a Chief of Mission.

(j) “Security Policy Board” means the Board established by the President to consider, coordinate, and recommend policy directives for U.S. security policies, procedures, and practices.

(k) “Special access program” has the meaning provided in section 4.1 of Executive Order No. 12958, or any successor order.

**Sec. 1.2. Access to Classified Information.** (a) No employee shall be granted access to classified information unless that employee has been determined to be eligible in accordance with this order and to possess a need-to-know.

(b) Agency heads shall be responsible for establishing and maintaining an effective program to ensure that access to classified information by each employee is clearly consistent with the interests of the national security.

(c) Employees shall not be granted access to classified information unless they:

(1) have been determined to be eligible for access under section 3.1 of this order by agency heads or designated officials based upon a favorable adjudication of an appropriate investigation of the employee's background;

(2) have a demonstrated need-to-know; and

(3) have signed an approved nondisclosure agreement.

(d) All employees shall be subject to investigation by an appropriate government authority prior to being granted access to classified information and at any time during the period of access to ascertain whether they continue to meet the requirements for access.

(e)(1) All employees granted access to classified information shall be required as a condition of such access to provide to the employing agency written consent permitting access by an authorized investigative agency, for such time as access to classified information is maintained and for a period of 3 years thereafter, to:

(A) relevant financial records that are maintained by a financial institution as defined in 31 U.S.C. 5312(a) or by a holding company as defined in section 1101(6) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401);

(B) consumer reports pertaining to the employee under the Fair Credit Reporting Act (15 U.S.C. 1681a); and

(C) records maintained by commercial entities within the United States pertaining to any travel by the employee outside the United States.

(2) Information may be requested pursuant to employee consent under this section where:

(A) there are reasonable grounds to believe, based on credible information, that the employee or former employee is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

(B) information the employing agency deems credible indicates the employee or former employee has incurred excessive indebtedness or has acquired a level of affluence that cannot be explained by other

information; or

(C) circumstances indicate the employee or former employee had the capability and opportunity to disclose classified information that is known to have been lost or compromised to a foreign power or an agent of a foreign power.

(3) Nothing in this section shall be construed to affect the authority of an investigating agency to obtain information pursuant to the Right to Financial Privacy Act, the Fair Credit Reporting Act or any other applicable law.

**Sec. 1.3. *Financial Disclosure.*** (a) Not later than 180 days after the effective date of this order, the head of each agency that originates, handles, transmits, or possesses classified information shall designate each employee, by position or category where possible, who has a regular need for access to classified information that, in the discretion of the agency head, would reveal:

(1) the identity of covert agents as defined in the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421);

(2) technical or specialized national intelligence collection and processing systems that, if disclosed in an unauthorized manner, would substantially negate or impair the effectiveness of the system;

(3) the details of:

(A) the nature, contents, algorithm, preparation, or use of any code, cipher, or cryptographic system or;

(B) the design, construction, functioning, maintenance, or repair of any cryptographic equipment; but not including information concerning the use of cryptographic equipment and services;

(4) particularly sensitive special access programs, the disclosure of which would substantially negate or impair the effectiveness of the information or activity involved; or

(5) especially sensitive nuclear weapons design information (but only for those positions that have been certified as being of a high degree of importance or sensitivity, as described in section 145(f) of the Atomic Energy Act of 1954, as amended).

(b) An employee may not be granted access, or hold a position designated as requiring access, to information described in subsection (a) unless, as a condition of access to such information, the employee:

(1) files with the head of the agency a financial disclosure report, including information with respect to the spouse and dependent children of the employee, as part of all background investigations or reinvestigations;

(2) is subject to annual financial disclosure requirements, if selected by the agency head; and

(3) files relevant information concerning foreign travel, as determined by the Security Policy Board.

(c) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop procedures for the implementation of this section, including a standard financial disclosure form for use by employees under subsection (b) of this section, and agency heads shall identify certain employees, by position or category, who are subject to annual financial disclosure.

**Sec. 1.4. *Use of Automated Financial Record Data Bases.*** As part of all investigations and reinvestigations described in section 1.2(d) of this order, agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, transactions under \$10,000 that are reported as possible money laundering violations, and records of foreign travel.

**Sec. 1.5. *Employee Education and Assistance.*** The head of each agency that grants access to classified information shall establish a program for employees with access to classified information to: (a) educate employees about individual responsibilities under this order; and (b) inform employees about guidance and assistance available concerning issues that may affect their eligibility for access to classified information, including sources of assistance for employees who have questions or concerns about financial matters, mental health, or substance abuse.

## PART 2—ACCESS ELIGIBILITY POLICY AND PROCEDURE

**Sec. 2.1. *Eligibility Determinations.*** (a) Determinations of eligibility for access to classified information shall be based on criteria established under this order. Such determinations are separate from suitability determinations with respect to the hiring or retention of persons for employment by the government or any other personnel actions.

(b) The number of employees that each agency determines are eligible for access to classified information shall be kept to the minimum required for the conduct of agency functions.

(1) Eligibility for access to classified information shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas when the employee has no need for access and access to classified information may reasonably be prevented. Where circumstances indicate employees may be inadvertently exposed to classified information in the course of their duties, agencies are authorized to grant or deny, in their discretion, facility access approvals to such employees based on an appropriate level of investigation as determined by each agency.

(2) Except in agencies where eligibility for access is a mandatory condition of employment, eligibility for access to classified information shall only be requested or granted based on a demonstrated, foreseeable need for access. Requesting or approving eligibility in excess of actual requirements is prohibited.

(3) Eligibility for access to classified information may be granted where there is a temporary need for access, such as one-time participation in a classified project, provided the investigative standards established under this order have been satisfied. In such cases, a fixed date or event for expiration shall be identified and access to classified information shall be limited to information related to the particular project or assignment.

(4) Access to classified information shall be terminated when an employee no longer has a need for access.

**Sec. 2.2. *Level of Access Approval.*** (a) The level at which an access approval is granted for an employee shall be limited, and relate directly, to the level of classified information for which there is a need for access. Eligibility for access to a higher level of classified information includes eligibility for access to information classified at a lower level.

(b) Access to classified information relating to a special access program shall be granted in accordance with procedures established by the head of the agency that created the program or, for programs

pertaining to intelligence activities (including special activities but not including military operational, strategic, and tactical programs) or intelligence sources and methods, by the Director of Central Intelligence. To the extent possible and consistent with the national security interests of the United States, such procedures shall be consistent with the standards and procedures established by and under this order.

**Sec. 2.3 *Temporary Access to Higher Levels.*** (a) An employee who has been determined to be eligible for access to classified information based on favorable adjudication of a completed investigation may be granted temporary access to a higher level where security personnel authorized by the agency head to make access eligibility determinations find that such access:

(1) is necessary to meet operational or contractual exigencies not expected to be of a recurring nature;

(2) will not exceed 180 days; and

(3) is limited to specific, identifiable information that is made the subject of a written access record.

(b) Where the access granted under subsection (a) of this section involves another agency's classified information, that agency must concur before access to its information is granted.

**Sec. 2.4. *Reciprocal Acceptance of Access Eligibility Determinations.*** (a) Except when an agency has substantial information indicating that an employee may not satisfy the standards in section 3.1 of this order, background investigations and eligibility determinations conducted under this order shall be mutually and reciprocally accepted by all agencies.

(b) Except where there is substantial information indicating that the employee may not satisfy the standards in section 3.1 of this order, an employee with existing access to a special access program shall not be denied eligibility for access to another special access program at the same sensitivity level as determined personally by the agency head or deputy agency head, or have an existing access eligibility readjudicated, so long as the employee has a need for access to the information involved.

(c) This section shall not preclude agency heads from establishing additional, but not duplicative, investigative or adjudicative procedures for a special access program or for candidates for detail or assignment to their agencies, where such procedures are required in exceptional circumstances to protect the national security.

(d) Where temporary eligibility for access is granted under sections 2.3 or 3.3 of this order or where the determination of eligibility for access is conditional, the fact of such temporary or conditional access shall be conveyed to any other agency that considers affording the employee access to its information.

**Sec. 2.5. *Specific Access Requirement.*** (a) Employees who have been determined to be eligible for access to classified information shall be given access to classified information only where there is a need-to-know that information.

(b) It is the responsibility of employees who are authorized holders of classified information to verify that a prospective recipient's eligibility for access has been granted by an authorized agency official and to ensure that a need-to-know exists prior to allowing such access, and to challenge requests for access that do not appear well-founded.

**Sec. 2.6. *Access by Non-United States Citizens.*** (a) Where there are compelling reasons in furtherance of an agency mission, immigrant alien and foreign national employees who possess a special expertise may, in the discretion of the agency, be granted limited access to classified information only for specific programs, projects, contracts, licenses, certificates, or grants for which there is a need for access. Such individuals shall not be eligible for access to any greater level of classified information than the United



States Government has determined may be releasable to the country of which the subject is currently a citizen, and such limited access may be approved only if the prior 10 years of the subject's life can be appropriately investigated. If there are any doubts concerning granting access, additional lawful investigative procedures shall be fully pursued.

(b) Exceptions to these requirements may be permitted only by the agency head or the senior agency official designated under section 6.1 of this order to further substantial national security interests.

**Section 3.5 was added by EO 13467**, and provides that an individual who has been determined to be eligible for or who currently has access to classified information shall be subject to continuous evaluation under standards (including, but not limited to, the frequency of such evaluation) as determined by the Director of National Intelligence."

### **•EO 12829 - National Industrial Security Program**

This order establishes a National Industrial Security Program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. To promote our national interests, the United States Government issues contracts, licenses, and grants to nongovernment organizations. When these arrangements require access to classified information, the national security requires that this information be safeguarded in a manner equivalent to its protection within the executive branch of Government. The national security also requires that our industrial security program promote the economic and technological interests of the United States. Redundant, overlapping, or unnecessary requirements impede those interests. Therefore, the National Industrial Security Program shall serve as a single, integrated, cohesive industrial security program to protect classified information and to preserve our Nation's economic and technological interests.

#### Part 1. Establishment and policy

**Section 101. Establishment.** (a) There is established a National Industrial Security Program. The purpose of this program is to safeguard classified information that may be released or has been released to current, prospective, or former contractors, licensees, or grantees of United States agencies. For the purposes of this order, the terms "contractor, licensee, or grantee" means current, prospective, or former contractors, licensees, or grantees of United States agencies. The National Industrial Security Program shall be applicable to all executive branch departments and agencies.

(b) The National Industrial Security Program shall provide for the protection of information classified pursuant to Executive Order No. 12356 of April 2, 1982, or its successor, and the Atomic Energy Act of 1954, as amended.

(c) For the purposes of this order, the term "contractor" does not include individuals engaged under personal services contracts.

**Sec. 203. Implementation.** (a) The head of each agency that enters into classified contracts, licenses, or grants shall designate a senior agency official to direct and administer the agency's implementation and compliance with the National Industrial Security Program.

(b) Agency implementing regulations, internal rules, or guidelines shall be consistent with this order, its implementing directives, and the Manual. Agencies shall issue these regulations, rules, or guidelines no later than 180 days from the issuance of the Manual. They may incorporate all or portions of the Manual by reference.

(c) Each agency head or the senior official designated under paragraph (a) above shall take appropriate

and prompt corrective action whenever a violation of this order, its implementing directives, or the Manual occurs.

(d) The senior agency official designated under paragraph (a) above shall account each year for the costs within the agency associated with the implementation of the National Industrial Security Program. These costs shall be reported to the Director of the Information Security Oversight Office, who shall include them in the reports to the President prescribed by this order.

(e) The Secretary of Defense, with the concurrence of the Administrator of General Services, the Administrator of the National Aeronautics and Space Administration, and such other agency heads or officials who may be responsible, shall amend the Federal Acquisition Regulation to be consistent with the implementation of the National Industrial Security Program.

(f) All contracts, licenses, or grants that involve access to classified information and that are advertised or proposed following the issuance of agency regulations, rules, or guidelines described in paragraph (b) above shall comply with the National Industrial Security Program. To the extent that is feasible, economical, and permitted by law, agencies shall amend, modify, or convert preexisting contracts, licenses, or grants, or previously advertised or proposed contracts, licenses, or grants, that involve access to classified information for operation under the National Industrial Security Program. Any direct inspection or monitoring of contractors, licensees, or grantees specified by this order shall be carried out pursuant to the terms of a contract, license, grant, or regulation.

**•EO 12564 - Drug-Free Federal Workplace**

I, RONALD REAGAN, President of the United States of America, find that:

Drug use is having serious adverse effects upon a significant proportion of the national work force and results in billions of dollars of lost productivity each year;

The Federal government, as an employer, is concerned with the well-being of its employees, the successful accomplishment of agency missions, and the need to maintain employee productivity;

The Federal government, as the largest employer in the Nation, can and should show the way towards achieving drug-free workplaces through a program designed to offer drug users a helping hand and, at the same time, demonstrating to drug users and potential drug users that drugs will not be tolerated in the Federal workplace;

The profits from illegal drugs provide the single greatest source of income for organized crime, fuel violent street crime, and otherwise contribute to the breakdown of our society;

The use of illegal drugs, on or off duty, by Federal employees is inconsistent not only with the law-abiding behavior expected of all citizens, but also with the special trust placed in such employees as servants of the public;

Federal employees who use illegal drugs, on or off duty, tend to be less productive, less reliable, and prone to greater absenteeism than their fellow employees who do not use illegal drugs;

The use of illegal drugs, on or off duty, by Federal employees impairs the efficiency of Federal departments and agencies, undermines public confidence in them, and makes it more difficult for other employees who do not use illegal drugs to perform their jobs effectively. The use of illegal drugs, on or off duty, by Federal employees also can pose a serious health and safety threat to members of the public and to other Federal employees;

The use of illegal drugs, on or off duty, by Federal employees in certain positions evidences less than the complete reliability, stability, and good judgment that is consistent with access to sensitive information and creates the possibility of coercion, influence, and irresponsible action under pressure that may pose a serious risk to national security, the public safety, and the effective enforcement of the law; and

Federal employees who use illegal drugs must themselves be primarily responsible for changing their behavior and, if necessary, begin the process of rehabilitating themselves.

By the authority vested in me as President by the Constitution and laws of the United States of America, including section 3301(2) of [Title 5 of the United States Code, section 7301](#) of Title 5 of the United States Code, [section 290ee-1 of Title 42 of the United States Code](#), deeming such action in the best interests of national security, public health and safety, law enforcement and the efficiency of the Federal service, and in order to establish standards and procedures to ensure fairness in achieving a drug-free Federal workplace and to protect the privacy of Federal employees, it is hereby ordered as follows:

**Section 1.** *Drug-Free Workplace.*

- (a) Federal employees are required to refrain from the use of illegal drugs.
- (b) The use of illegal drugs by Federal employees, whether on duty or off duty, is contrary to the efficiency of the service.
- (c) Persons who use illegal drugs are not suitable for Federal employment.**

**Sec. 2.** *Agency Responsibilities.*

- (a) The head of each Executive agency shall develop a plan for achieving the objective of a drug-free workplace with due consideration of the rights of the government, the employee, and the general public.
- (b) Each agency plan shall include:
  - (1) A statement of policy setting forth the agency's expectations regarding drug use and the action to be anticipated in response to identified drug use;
  - (2) Employee Assistance Programs emphasizing high level direction, education, counseling, referral to rehabilitation, and coordination with available community resources;
  - (3) Supervisory training to assist in identifying and addressing illegal drug use by agency employees;
  - (4) Provision for self-referrals as well as supervisory referrals to treatment with maximum respect for individual confidentiality consistent with safety and security issues; and
  - (5) Provision for identifying illegal **drug** users, including **testing** on a controlled and carefully monitored basis in accordance with this Order.

### **Sec. 3. Drug Testing Programs.**

(a) The head of each Executive agency shall establish a program to test for the use of illegal drugs by employees in sensitive positions. The extent to which such employees are tested and the criteria for such testing shall be determined by the head of each agency, based upon the nature of the agency's mission and its employees' duties, the efficient use of agency resources, and the danger to the public health and safety or national security that could result from the failure of an employee adequately to discharge his or her position.

(b) The head of each Executive agency shall establish a program for voluntary employee **drug testing**.

(c) In addition to the testing authorized in subsections (a) and (b) of this section, the head of each Executive agency is authorized to test an employee for illegal drug use under the following circumstances:

- (1) When there is a reasonable suspicion that any employee uses illegal drugs;
  - (2) In an examination authorized by the agency regarding an accident or unsafe practice; or
  - (3) As part of or as a follow-up to counseling or rehabilitation for illegal drug use through an Employee Assistance Program.
- (d) The head of each Executive agency is authorized to test any applicant for illegal drug use.

### **Sec. 4. Drug Testing Procedures.**

(a) Sixty days prior to the implementation of a **drug testing** program pursuant to this Order, agencies shall notify employees that testing for use of illegal drugs is to be conducted and that they may seek counseling and rehabilitation and inform them of the procedures for obtaining such assistance through the agency's Employee Assistance Program. Agency **drug testing** programs already ongoing are exempted from the 60-day notice requirement. Agencies may take action under section 3(c) of this Order without reference to the 60-day notice period.

**\*32891** (b) Before conducting a **drug test**, the agency shall inform the employee to be tested of the opportunity to submit medical documentation that may support a legitimate use for a specific **drug**.

(c) **Drug testing** programs shall contain procedures for timely submission of requests for retention of records and specimens; procedures for retesting; and procedures, consistent with applicable law, to protect the confidentiality of test results and related medical and rehabilitation records. Procedures for providing urine specimens must allow individual privacy, unless the agency has reason to believe that a particular individual may alter or substitute the specimen to be provided.

(d) The Secretary of Health and Human Services is authorized to promulgate scientific and technical guidelines for **drug testing** programs, and agencies shall conduct their **drug testing** programs in accordance with these guidelines once promulgated.

### **Sec. 5. Personnel Actions.**

(a) Agencies shall, in addition to any appropriate personnel actions, refer any employee who is found to

use illegal drugs to an Employee Assistance Program for assessment, counseling, and referral for treatment or rehabilitation as appropriate.

(b) Agencies shall initiate action to discipline any employee who is found to use illegal drugs, *provided that* such action is not required for an employee who:

(1) Voluntarily identifies himself as a user of illegal drugs or who volunteers for **drug testing** pursuant to section 3(b) of this Order, prior to being identified through other means;

(2) Obtains counseling or rehabilitation through an Employee Assistance Program; and

(3) Thereafter refrains from using illegal drugs.

(c) Agencies shall not allow any employee to remain on duty in a sensitive position who is found to use illegal drugs, prior to successful completion of rehabilitation through an Employee Assistance Program. However, as part of a rehabilitation or counseling program, the head of an Executive agency may, in his or her discretion, allow an employee to return to duty in a sensitive position if it is determined that this action would not pose a danger to public health or safety or the national security.

(d) Agencies shall initiate action to remove from the service any employee who is found to use illegal drugs and:

(1) Refuses to obtain counseling or rehabilitation through an Employee Assistance Program; or

(2) Does not thereafter refrain from using illegal drugs.

(e) The results of a **drug test** and information developed by the agency in the course of the **drug testing** of the employee may be considered in processing any adverse action against the employee or for other administrative purposes. Preliminary test results may not be used in an administrative proceeding unless they are confirmed by a second analysis of the same sample or unless the employee confirms the accuracy of the initial test by admitting the use of illegal drugs.

(f) The determination of an agency that an employee uses illegal drugs can be made on the basis of any appropriate evidence, including direct observation, a criminal conviction, administrative inquiry, or the results of an authorized **testing** program. Positive **drug test** results may be rebutted by other evidence that an employee has not used illegal drugs.

(g) Any action to discipline an employee who is using illegal drugs (including removal from the service, if appropriate) shall be taken in compliance with otherwise applicable procedures, including the Civil Service Reform Act.

(h) **Drug testing** shall not be conducted pursuant to this Order for the purpose of gathering evidence for use in criminal proceedings. Agencies are not required to report to the Attorney General for investigation or prosecution any information, allegation, or evidence relating to violations of Title 21 of the United States Code received as a result of the operation of **drug testing** programs established pursuant to this Order.

## **Sec. 6. Coordination of Agency Programs.**

(a) The Director of the Office of Personnel Management shall:

- (1) Issue government-wide guidance to agencies on the implementation of the terms of this Order;
  - (2) Ensure that appropriate coverage for drug abuse is maintained for employees and their families under the Federal Employees Health Benefits Program;
  - (3) Develop a model Employee Assistance Program for Federal agencies and assist the agencies in putting programs in place;
  - (4) In consultation with the Secretary of Health and Human Services, develop and improve training programs for Federal supervisors and managers on illegal drug use; and
  - (5) In cooperation with the Secretary of Health and Human Services and heads of Executive agencies, mount an intensive drug awareness campaign throughout the Federal work force.
- (b) The Attorney General shall render legal advice regarding the implementation of this Order and shall be consulted with regard to all guidelines, regulations, and policies proposed to be adopted pursuant to this Order.
- (c) Nothing in this Order shall be deemed to limit the authorities of the Director of Central Intelligence under the National Security Act of 1947, as amended, or the statutory authorities of the National Security Agency or the Defense Intelligence Agency. Implementation of this Order within the [Intelligence Community, as defined in Executive Order No. 12333](#), shall be subject to the approval of the head of the affected agency.

## **Sec. 7. Definitions.**

- (a) This Order applies to all agencies of the Executive Branch.
- (b) For purposes of this Order, the term “agency” means an Executive agency, as defined in [5 U.S.C. 105](#); the Uniformed Services, as defined in [5 U.S.C. 2101\(3\)](#) (but excluding the armed forces as defined by [5 U.S.C. 2101\(2\)](#)); or any other employing unit or authority of the Federal government, except the United States Postal Service, the Postal Rate Commission, and employing units or authorities in the Judicial and Legislative Branches.
- (c) For purposes of this Order, the term “illegal drugs” means a controlled substance included in Schedule I or II, as defined by [section 802\(6\) of Title 21 of the United States Code](#), the possession of which is unlawful under chapter 13 of that Title. The term “illegal drugs” does not mean the use of a controlled substance pursuant to a valid prescription or other uses authorized by law.
- (d) For purposes of this Order, the term “employee in a sensitive position” refers to:
- (1) An employee in a position that an agency head designates Special Sensitive, Critical-Sensitive, or Noncritical-Sensitive under Chapter 731 of the Federal Personnel Manual or an employee in a position that an agency head designates as sensitive in accordance with [Executive Order No. 10450](#), as amended;
  - (2) An employee who has been granted access to classified information or may be granted access to classified information pursuant to a determination of trustworthiness by an agency head under Section 4 of [Executive Order No. 12356](#);
  - (3) Individuals serving under Presidential appointments;

(4) Law enforcement officers as defined in [5 U.S.C. 8331\(20\)](#); and

(5) Other positions that the agency head determines involve law enforcement, national security, the protection of life and property, public health or safety, or other functions requiring a high degree of trust and confidence.

(e) For purposes of this Order, the term “employee” means all persons appointed in the Civil Service as described in [5 U.S.C. 2105](#) (but excluding persons appointed in the armed services as defined in [5 U.S.C. 2102\(2\)](#)).

(f) For purposes of this Order, the term “Employee Assistance Program” means agency-based counseling programs that offer assessment, short-term counseling, and referral services to employees for a wide range of drug, alcohol, and mental health programs that affect employee job performance. Employee Assistance Programs are responsible for referring drug-using employees for rehabilitation and for monitoring employees' progress while in treatment.

**Sec. 8. *Effective Date.*** This Order is effective immediately.

**•EO 12333 - *United States Intelligence Activities (as amended by Executive Orders 13284 (2003), 13355 (2004), and 13470 (2008))***

*\*Note section 1.5(h) requires the heads of executive branch departments and agencies to inform the Attorney General, either directly or through the Federal Bureau of Investigation, and the Director of National Intelligence of clandestine collection of foreign intelligence and counterintelligence activities inside the United States not coordinated with the Federal Bureau of Investigation.*

**1.5 *Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies.*** The heads of all departments and agencies shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Provide all programmatic and budgetary information necessary to support the Director in developing the National Intelligence Program;

(c) Coordinate development and implementation of intelligence systems and architectures and, as appropriate, operational systems and architectures of their departments, agencies, and other elements with the Director to respond to national intelligence requirements and all applicable information sharing and security guidelines, information privacy, and other legal requirements;

(d) Provide, to the maximum extent permitted by law, subject to the availability of appropriations and not inconsistent with the mission of the department or agency, such further support to the Director as the Director may request, after consultation with the head of the department or agency, for the performance of the Director's functions;

- (e) Respond to advisory tasking from the Director under section 1.3(b)(18) of this order to the greatest extent possible, in accordance with applicable policies established by the head of the responding department or agency;
- (f) Ensure that all elements within the department or agency comply with the provisions of Part 2 of this order, regardless of Intelligence Community affiliation, when performing foreign intelligence and counterintelligence functions;
- (g) Deconflict, coordinate, and integrate all intelligence activities in accordance with section 1.3(b)(20), and intelligence and other activities in accordance with section 1.3(b)(21) of this order;
- (h) Inform the Attorney General, either directly or through the Federal Bureau of Investigation, and the Director of clandestine collection of foreign intelligence and counterintelligence activities inside the United States not coordinated with the Federal Bureau of Investigation;**
- (i) Pursuant to arrangements developed by the head of the department or agency and the Director of the Central Intelligence Agency and approved by the Director, inform the Director and the Director of the Central Intelligence Agency, either directly or through his designee serving outside the United States, as appropriate, of clandestine collection of foreign intelligence collected through human sources or through human-enabled means outside the United States that has not been coordinated with the Central Intelligence Agency; and
- (j) Inform the Secretary of Defense, either directly or through his designee, as appropriate, of clandestine collection of foreign intelligence outside the United States in a region of combat or contingency military operations designated by the Secretary of Defense, for purposes of this paragraph, after consultation with the Director of National Intelligence.

1.6 *Heads of Elements of the Intelligence Community.* The heads of elements of the Intelligence Community shall:

(b) Report to the Attorney General possible violations of Federal criminal laws by employees and of specified Federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department, agency, or establishment concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures. (*Writer's note, see also MOU: Reporting of Information Concerning Federal Crimes* (signed by Intelligence Community agencies in 1995)).

**•EO 10577 - Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service**

SECTION 101. The Civil Service Rules are hereby amended to read as follows:

**RULE I—COVERAGE AND DEFINITIONS**

SEC. 1.1 *Positions and employees affected by these Rules.* These Rules shall apply to all positions in the competitive service and to all incumbents of such positions. Except as expressly provided in the Rule concerned, these Rules shall not apply to positions and employees in the excepted service.

SEC. 1.2 *Extent of the competitive service.* The competitive service shall include: (a) All civilian positions in the executive branch of the Government unless specifically excepted therefrom by or pursuant to



statute or by the Civil Service Commission (hereafter referred to in these Rules as the Commission) under section 6.1 of Rule VI; and (b) all positions in the legislative and judicial branches of the Federal Government and in the Government of the District of Columbia which are specifically made subject to the civil-service laws by statute. The Commission is authorized and directed to determine finally whether a position is in the competitive service.

SEC. 1.3 *Definitions.* As used in these Rules:

(a) 'Competitive service' shall have the same meaning as the words 'classified service', or 'classified (competitive) service', or 'classified civil service' as defined in existing statutes and executive orders.

(b) 'Competitive position' shall mean a position in the competitive service.

(c) 'Competitive status' shall mean basic eligibility to be noncompetitively selected to fill a vacancy in a competitive position. A competitive status shall be acquired by career-conditional or career appointment through open competitive examination upon satisfactory completion of a probationary period, or may be granted by statute, executive order, or the Civil Service Rules without competitive examination. A person with competitive status may be promoted, transferred, reassigned, reinstated, or demoted without taking an open competitive examination, subject to the conditions prescribed by the Civil Service Rules and Regulations.

(d) An employee shall be considered as being in the competitive service when he has a competitive status and occupies a competitive position unless he is serving under a temporary appointment: *Provided*, That an employee who is in the competitive service at the time his position is first listed under Schedule A, B, or C shall be considered as continuing in the competitive service as long as he continues to occupy such position.

(e) 'Tenure' shall mean the period of time an employee may reasonably expect to serve under his current appointment. Tenure shall be granted and governed by the type of appointment under which an employee is currently serving without regard to whether he has a competitive status or whether his appointment is to a competitive position or an excepted position.

SEC. 1.4 *Extent of the excepted service.* (a) The excepted service shall include all civilian positions in the executive branch of the Government which are specifically excepted from the requirements of the Civil Service Act or from the competitive service by or pursuant to statute or by the Commission under section 6.1 of Rule VI.

(b) 'Excepted service' shall have the same meaning as the words 'unclassified service', or 'unclassified civil service', or 'positions outside the competitive civil service' as used in existing statutes and executive orders.

(c) 'Excepted position' shall have the same meaning as 'unclassified position', or 'position excepted by law', or 'position excepted by executive order', or 'position excepted by Civil Service Rule', or 'position outside the competitive service' as used in existing statutes and executive orders.

## RULE V—REGULATIONS, INVESTIGATION, AND ENFORCEMENT

SEC. 5.1 *Regulations.* (a) The Commission is authorized and directed to promulgate and enforce such regulations as may be necessary to carry out the provisions of the Civil Service Act and Rules, the Veterans' Preference Act, and all other applicable statutes or executive orders imposing responsibilities on the Commission.

(b) The Commission is authorized, whenever there shall be practical difficulties and unnecessary hardships in complying with the strict letter of its regulations, to grant a variation from the strict letter of the regulations if such variation is within the spirit of the regulations, and the efficiency of the Government and the integrity of the competitive service are protected and promoted: *Provided*, That whenever such a variation is granted the Commission shall record in the minutes of its proceedings (1) the particular practical difficulty or hardship involved, (2) what is permitted in lieu of what is required by regulation, (3) the circumstances which protect or promote the efficiency of the Government and the integrity of the competitive service, and (4) a statement limiting the application of the variation to the continuation of the conditions which gave rise to the variation: *Provided further*, That similar variations shall be granted whenever similar conditions exist. All minutes approved under authority of this section shall be published in the Commission's annual reports.

*SEC. 5.2 Authority of the Commission to make investigations.* The Commission may make appropriate investigations to secure enforcement of the Civil Service Act, Rules, and Regulations, including investigation of the qualifications and suitability of applicants for positions in the competitive service. It may require appointments to be made subject to investigation to enable the Commission to determine, after appointment, that the requirements of law or the Civil Service Rules and Regulations have been met. Whenever the Commission finds that an employee serving under such an appointment is disqualified for Federal employment, it may instruct the agency to remove him, or to suspend him pending an appeal from the Commission's finding: *Provided*, That when an agency removes or suspends an employee pursuant to the Commission's instructions, and the Commission, on the basis of new evidence or on appeal, subsequently reverses the initial decision as to the employee's qualifications and suitability, the agency shall, upon request of the Commission, restore the employee to duty.

*SEC. 5.3 Officers and employees to furnish testimony.* All officers and employees in the executive branch, and applicants or eligibles for positions therein, shall give to the Commission or its authorized representatives all information and testimony in regard to matters inquired of arising under the laws, rules, and regulations administered by the Commission. Whenever required by the Commission, such persons shall subscribe such testimony and make oath or affirmation thereto before an officer authorized by law to administer oaths.

*SEC. 5.4 Enforcement authority of the Commission.* (a) Whenever the Commission finds that any person has been appointed to or is holding a position in violation of the Civil Service Act, Rules or Regulations, or that any officer or employee in the executive branch has violated this order or any of the laws, rules or regulations administered by the Commission, it is authorized, after giving due notice and opportunity for explanation to the officer or employee and the agency concerned, to certify the facts to the proper appointing officer with specific instructions as to discipline or dismissal or other corrective action.

(b) Whenever the Commission finds that any officer or employee in the executive branch has failed to adhere to established policies, regulations, and standards relating to personnel management subject to the jurisdiction of the Commission, it shall instruct the agency head to take corrective action.

(c) Whenever, on the basis of an appeal by an employee, the Commission finds that its regulations prescribing procedures to be followed by agencies in connection with adverse actions for disciplinary reasons have not been followed, or that adverse action has been taken for political reasons except as may be required by law, or resulted from discrimination because of marital status, it shall instruct the agency to restore the employee to duty.

(d) Whenever the Commission issues specific instructions as to discipline or dismissal of an officer or employee, or to restore an officer or employee to duty, the appointing officer concerned shall comply with

the Commission's instructions.

(e) If the appointing officer fails to carry out the instructions of the Commission issued under section 4(a) of this Rule, the Commission shall certify the facts to the head of the agency concerned. If the head of the agency fails to carry out the instructions of the Commission within ten days after receipt thereof, the Commission shall certify the facts to the Comptroller General of the United States, and shall furnish a copy of such certification to the head of the agency concerned; and thereafter no payment shall be made of the salary or wages accruing to the employee concerned.

## RULE VI—EXCEPTIONS FROM THE COMPETITIVE SERVICE

SEC. 6.1 *Authority to except positions from the competitive service.* (a) The Commission is authorized to except positions from the competitive service whenever it determines that appointments thereto through competitive examination are not practicable. Upon the recommendation of the agency concerned, it may also except positions which are of a confidential or policy-determining character. Such exceptions from the competitive service shall be effective upon publication thereof in the FEDERAL REGISTER. Positions excepted by the Commission shall be listed in Schedule A, B, or C as provided for in section 6.2 of this Rule, and shall also be listed in the Commission's annual report for the fiscal year in which the exceptions are made.

(b) The Commission shall decide whether the duties of any particular position are such that it may be filled as an excepted position under the appropriate schedule.

SEC. 6.2 *Schedules of excepted positions.* The Commission shall list positions that it excepts from the competitive service in Schedules A, B, and C, which schedules shall constitute parts of this Rule, as follows:

*Schedule A.* Positions other than those of a confidential or policy-determining character for which it is not practicable to examine shall be listed in Schedule A.

*Schedule B.* Positions other than those of a confidential or policy-determining character for which it is not practicable to hold a competitive examination shall be listed in Schedule B. Appointments to these positions shall be subject to such noncompetitive examination as may be prescribed by the Commission.

*Schedule C.* Positions of a confidential or policy-determining character shall be listed in Schedule C.

SEC. 6.3 *Method of filling excepted positions and status of incumbents.* (a) The head of an agency may fill excepted positions by the appointment of persons without civil service eligibility or competitive status and such persons shall not acquire competitive status by reason of such appointment: *Provided*, That the Commission, in its discretion, may by regulation prescribe conditions under which excepted positions may be filled in the same manner as competitive positions are filled and conditions under which persons so appointed may acquire a competitive status in accordance with the Civil Service Rules and Regulations.

(b) To the extent permitted by law and the provisions of this Rule, appointments and position changes in the excepted service shall be made in accordance with such regulations and practices as the head of the agency concerned finds necessary.

SEC. 6.4 *Removal of incumbents of excepted positions.* Except as may be required by statute, the Civil Service Rules and Regulations shall not apply to removals from positions listed in Schedules A and C or from positions excepted from the competitive service by statute. The Civil Service Rules and Regulations shall apply to removals from positions listed in Schedule B of persons who have competitive status.

SEC. 6.5 *Assignment of excepted employees.* No person who is serving under an excepted appointment shall be assigned to the work of a position in the competitive service without prior approval of the Commission.

SEC. 6.6 *Revocation of exceptions.* The Commission may remove any position from or may revoke in whole or in part any provision of Schedule A or B, and, with the concurrence of the agency concerned, may remove any position from or may revoke in whole or in part any provision of Schedule C. Such changes shall become effective upon publication thereof in the FEDERAL REGISTER.

•**EO 10450 - Security Requirements for Government Employment** (See generally Title 5 US Code § 7311: *Employment Limitations, Loyalty and Striking*)

*\*Note this order provides there shall be referred promptly to the Federal Bureau of Investigation all investigations being conducted by any other agencies which develop information indicating that an individual may have been subjected to coercion, influence, or pressure to act contrary to the interests of the national security, or information relating to any of the matters described in subdivisions (2) through (7) of subsection (a) of section 8 of this order.*

WHEREAS the interests of the national security require that **all persons privileged to be employed in the departments and agencies of the Government**, shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States.

SEC. 2. The head of each department and agency of the Government shall be responsible for establishing and maintaining within his department or agency an effective program to insure that the employment and retention in employment of any civilian officer or employee within the department or agency is clearly consistent with the interests of the national security.

SEC. 3. (a) **The appointment of each civilian officer or employee in any department or agency of the Government shall be made subject to investigation.** The scope of the investigation shall be determined in the first instance according to the degree of adverse effect the occupant of the position sought to be filled could bring about, by virtue of the nature of the position, on the national security, but in no event shall the investigation include less than a national agency check (including a check of the fingerprint files of the Federal Bureau of Investigation), and written inquiries to appropriate local law-enforcement agencies, former employers and supervisors, references, and schools attended by the person under investigation: *Provided*, that upon request of the head of the department or agency concerned, the Civil Service Commission may, in its discretion, authorize such less investigation as may meet the requirements of the national security with respect to per-diem, intermittent, temporary, or seasonal employees, or aliens employed outside the United States. Should there develop at any stage of investigation information indicating that the employment of any such person may not be clearly consistent with the interests of the national security, there shall be conducted with respect to such person a full field investigation, or such less investigation as shall be sufficient to enable the head of the department or agency concerned to determine whether retention of such person is clearly consistent with the interests of the national security.

(b) **The head of any department or agency** shall designate, or cause to be designated, any position within his department or agency the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security as a sensitive position. Any position so designated shall be filled or occupied only by a person with respect to whom a full field investigation has

been conducted: *Provided*, that a person occupying a sensitive position at the time it is designated as such may continue to occupy such position pending the completion of a full field investigation, subject to the other provisions of this order: *And provided further*, that in case of emergency a sensitive position may be filled for a limited period by a person with respect to whom a full field preappointment investigation has not been completed if the head of the department or agency concerned finds that such action is necessary in the national interest, which finding shall be made a part of the records of such department or agency.

SEC. 8. (a) The investigations conducted pursuant to this order shall be designed to develop information as to whether the employment or retention in employment in the Federal service of the person being investigated is clearly consistent with the interests of the national security. Such information shall relate, but shall not be limited, to the following:

(1) Depending on the relation of the Government employment to the national security:

(i) Any behavior, activities, or associations which tend to show that the individual is not reliable or trustworthy.

(ii) Any deliberate misrepresentations, falsifications, or omissions of material facts.

(iii) Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, sexual perversion, or financial irresponsibility.

(iv) An adjudication of insanity, or treatment for serious mental or neurological disorder without satisfactory evidence of cure.

(v) Any facts which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause him to act contrary to the best interests of the national security.

(2) Commission of any act of sabotage, espionage, treason, or sedition, or attempts thereat or preparation therefore, or conspiring with, or aiding or abetting, another to commit or attempt to commit any act of sabotage, espionage, treason, or sedition.

(3) Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, or with an espionage or other secret agent or representative of a foreign nation, or any representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the government of the United States or the alteration of the form of government of the United States by unconstitutional means.

(4) Advocacy of use of force or violence to overthrow the government of the United States, or of the alteration of the form of government of the United States by unconstitutional means.

(5) Membership in, or affiliation or sympathetic association with, any foreign or domestic organization, association, movement, group, or combination of persons which is totalitarian, Fascist, Communist, or subversive, or which has adopted, or shows, a policy of advocating or approving the commission of acts of force or violence to the deny other persons their rights under the Constitution of the United States, or which seeks to alter the form of government of the United States by unconstitutional means.

(6) Intentional, unauthorized disclosure to any person of security information, or of other information disclosure of which is prohibited by law, or willful violation or disregard of security regulations.

(7) Performing or attempting to perform his duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

(b) The investigation of persons entering or employed in the competitive service shall primarily be the responsibility of the Civil Service Commission, except in cases in which the head of a department or agency assumes that responsibility pursuant to law or by agreement with the Commission. The Commission shall furnish a full investigative report to the department or agency concerned.

(c) The investigation of persons (including consultants, however employed), entering employment of, or employed by, the Government other than in the competitive service shall primarily be the responsibility of the employing department or agency. Departments and agencies without investigative facilities may use the investigative facilities of the Civil Service Commission, and other departments and agencies may use such facilities under agreement with the Commission.

(d) There shall be referred promptly to the Federal Bureau of Investigation all investigations being conducted by any other agencies which develop information indicating that an individual may have been subjected to coercion, influence, or pressure to act contrary to the interests of the national security, or information relating to any of the matters described in subdivisions (2) through (7) of subsection (a) of this section. In cases so referred to it, the Federal Bureau of Investigation shall make a full field investigation.

## **Presidential National Security Directives and Homeland Security Presidential Directives**

### **•*National Security Directive 42 - National Policy for the Security of National Security Telecommunications and Information Systems***

This Directive establishes initial objectives, policies, and an organizational structure to guide the conduct of activities to secure national security systems from exploitation; establishes a mechanism for policy development and dissemination; and assigns responsibilities for implementation. It is intended to ensure full participation and cooperation among the various existing centers of technical expertise throughout the Executive branch, and to promote a coherent and coordinated defense against the foreign intelligence threat to these systems. This Directive recognizes the special requirements for protection of intelligence sources and methods.

#### 8. The Heads of Executive Departments and Agencies shall:

- a. Be responsible for achieving and maintaining secure national security systems within their departments or agencies;
- b. Ensure that policies, procedures, guidelines, instructions, and standards issued pursuant to this Directive are implemented within their departments or agencies; and
- c. Provide to the NSTISSC, the Executive Agent, and the National Manager, as appropriate, such information as may be required to discharge responsibilities assigned herein, consistent with relevant law, Executive Order, and Presidential directive.

### **•*National Security Directive 63 - Single Scope Background Investigations***

- To eliminate redundant and costly investigative practices currently employed throughout the Executive branch, the President directed that the following minimum investigative scope and standards be adopted by all agencies and departments for access for Collateral Top Secret/National Security Information and Sensitive Compartmented Information.

#### **Scope**

Past ten (10) years or to age 18, whichever is less.

#### **Expansion of Investigation**

The investigation may be expanded as necessary, to resolve issues and/or address employment standards unique to individual agencies.

## **National Agency Check**

Checks on subject and spouse/cohabitant of investigative and criminal history files of the Federal Bureau of Investigation, including submission of fingerprint records on the subject, and such other national agencies (DCII, INS, OPM, CIA, etc.) as appropriate to the individual's background.

## **Subject Interview**

Required in all cases and shall be conducted by trained security, investigative, or counterintelligence personnel to ensure full investigative coverage.

An additional personal interview shall be conducted when necessary to resolve any significant information and/or inconsistencies developed during the investigation. In departments or agencies with policies sanctioning the use of the polygraph for personnel security purposes, the personal interview may include a polygraph examination, conducted by a qualified polygraph examiner.

## **Birth**

Independent certification of date and place of birth received directly from appropriate registration authority.

## **Citizenship**

Subject must be a U.S. citizen. Independent verification of citizenship received directly from appropriate registration authority. For foreign-born immediate family members, verification of citizenship or legal status is also required.

## **Education**

Independent verification of most recent or most significant claimed attendance and/or degree/diploma within the scope of investigation via sealed transcript received directly from the institution. If all education is outside of the investigative scope, the last education above high school level will be verified.

## **Employment**

Direct verification through records of all periods of employment within scope but in any event the most recent two (2) years. Personal interviews of two sources (supervisor/coworkers) for each employment of six months or more shall be attempted. In the event that no employment exceeds six months, interviews of supervisor/coworkers shall be attempted. All periods of unemployment in excess of sixty (60) days shall be verified through records and/or sources. All prior federal/military service and type of discharges shall be verified.

## **References**

Four required (at least three of which are developed). To the extent practical, all should have social knowledge of subject and collectively span the entire scope of the investigation.

As appropriated, additional interviews may include cohabitant(s), ex-spouses, and relative(s). Interviews with psychological/medical personnel are to be accomplished as required to resolve issues.



## **Neighborhood**

Interviews with neighbors for last five years if residence exceeds six months. Confirmation of current residence shall be accomplished regardless of length to include review of rental records if necessary. In the event no residence exceeds six months, interview of neighbors should be undertaken.

## **Credit**

Verification of the subject's financial status and credit habits of all locations where subject has resided, been employed, or attended school for six months or more for the last seven (7) years.

## **Local Agency Checks**

A check of appropriate Police records covering all locations where subject has resided, been employed, or attended school for six months or more during the scope of investigation, to include current residence regardless of duration. In the event that no residence, employment, or education exceeds six months, local agency checks should be performed.

## **Public Records**

Verification of divorce(s), bankruptcy, etc., and any other court (civil or criminal) actions to which subject has been or is a party within the scope of investigation, when known or developed.

## **Transferability**

Investigations satisfying the scope and standards specified above are transferable between agencies and shall be deemed to meet the investigative standards for access to collateral Top Secret/National Security Information and Sensitive Compartmented Information. No further investigation or reinvestigation prior to revalidation every five years will be undertaken unless the agency has substantial information indicating that the transferring individual may not satisfy eligibility standards for clearance or the agency head determines in writing that to accept the investigation would not be in the national security interest of the United States.

## **Notes**

Immediate family -- spouse, parents, brothers, sisters, children, and cohabitant of the individual requiring access.

## **•Presidential Decision Directive/NSC-12- Security Awareness and Reporting of Foreign Contacts**

This directive requires each department or agency to establish procedures, in consultation with the Department of Justice, which require its employees to report all contacts with individuals of any nationality, either within or outside the scope of the employee's official activities, in which:

- Illegal or unauthorized access is sought to classified or otherwise sensitive information.
- The employee is concerned that he/she may be the target of actual or attempted exploitation by a foreign entity.

**•National Security Presidential Directive 54/Homeland Security Presidential Directive 23 - Cybersecurity Policy**

-Among other things, this directive provides:

(1) Federal agencies shall protect the confidentiality, integrity, and availability of information stored, processed, and transmitted on their information systems, and ensure the authentication of access to such systems as required; and

(2) The heads of all Federal agencies, to the extent permitted by law and necessary for the effective implementation of the cybersecurity mission, shall support and collaborate with the Secretary of Homeland Security.

**•Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience**

-All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions. Such infrastructure shall be addressed in the plans and execution of the requirements in the National Continuity Policy.

**•Homeland Security Presidential Directive 12 - Policies for a Common Identification Standard for Federal Employees and Contractors**

There are wide variations in the quality and security of identification used to gain access to secure facilities where there is potential for terrorist attacks. In order to eliminate these variations, U.S. policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive mandates a federal standard for secure and reliable forms of identification.

## **Intelligence Community Directives**

### **•*Intelligence Community Directive 500 – Chief Information Officer***

-This ICD applies to the IC, as defined by the National Security Act of 1947, as amended, and other departments or agencies that may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the IC.

-This ICD sets forth the authorities and responsibilities of the Chief Information Officer of the Intelligence Community.

-Among other things, this ICD requires agencies, offices and elements of the IC, consistent with the standards promulgated for national security systems as authorized by law and directed by the President and the requirements for information security established by Subchapter III of FISMA, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of:

(1) Information collected or maintained by or on behalf of agencies, offices, and elements of the IC; or

(2) Information systems used or operated by or on behalf of an agency, office or element of the IC or by a contractor of an agency, office or element of the IC.

### **•*Intelligence Community Directive 503 - Information Technology Systems Security, Risk Management, Certification and Accreditation***

-This ICD applies to the IC, as defined by the National Security Act of 1947, as amended, and other departments or agencies that may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the IC.

-This policy implements strategic goals agreed upon in January 2007 by the IC Chief Information Officer (CIO), the Chief Information Officers of the Department of Defense (DoD), the Office of Management and Budget, and the National Institute of Standards and Technology (NIST). This ICD focuses on a more holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop trust across the intelligence community information technology enterprise through the use of common standards and reciprocally accepted certification and accreditation decisions.

## **D. POLICY**

### **1. Risk Management**

a. The principal goal of an IC element's information technology risk management process shall be to protect the element's ability to perform its mission, not just its information assets. Therefore, IC elements

shall consider risk management an essential management function, and shall ensure that it is tightly woven into the system development life cycle.

## **2. Accreditation**

a. Accreditation decisions are official management decisions that explicitly accept a defined level of risk associated with the operation of an information technology system at a particular level of security in a specific environment on behalf of an IC element.

## **3. Certification**

a. A security certification is the required comprehensive assessment of the management, operational, and technical security controls in an information technology system, or for a particular item of information technology, made in support of accreditation.

## **4. Reciprocity**

a. Elements of the IC shall make appropriate accreditation documentation available to other IC elements, and to the non-IC parts of the DoD generally, its Military Departments, Combatant Commands and Defense Agencies, and also to non-IC agencies of the Federal Government.

## **5. Interconnection**

a. Elements of the IC shall permit interconnections of accredited information technology systems with the accredited systems of other IC elements in accordance with standards for system interconnection published, issued and promulgated by the IC CIO. Information technology system interconnection standards published, issued, and promulgated for the IC by the IC CIO may include standards, policies and guidelines approved by either or both NIST and CNSS.

### **•*Intelligence Community Directive 700 - Protection of National Intelligence***

-This ICD applies to the IC, as defined by the National Security Act of 1947, as amended, and other departments or agencies that may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the IC.

1. This Directive establishes Intelligence Community (IC) policy for the protection of national intelligence, providing the framework for:

a. The protection of national intelligence and intelligence sources, methods, and activities; and the prevention of compromises, unauthorized disclosures, and misuses of national intelligence through coordinated CI and security activities;

b. Greater coordination and communication between CI and security activities of the IC to strengthen the ability to identify, deter, disrupt, mitigate, and counteract intelligence activities directed against United States (US) interests by foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities; and

c. Oversight of CI and security activities across the IC.

## **2. Heads of the IC elements shall:**

a. Protect national intelligence and intelligence sources, methods and activities from unauthorized disclosure, consistent with federal laws, regulations, Executive Orders and any other applicable policy.

b. Ensure CI and security elements within their organizations collaborate and share data and information as necessary, to protect national intelligence and intelligence sources, methods and activities. For IC elements where either CI or security is a departmental asset, the IC element head is responsible for ensuring that any IC-related concerns are communicated to the Department.

c. Implement, where applicable, internal CI and security policies, procedures, practices, and programs in accordance with IC policies and standards to ensure the appropriate identification, protection, handling, storage, access to, and dissemination of national intelligence.

d. Employ risk management principles to minimize the potential for unauthorized disclosure or compromise of national intelligence and intelligence sources, methods, and activities while maximizing the sharing of information.

e. Ensure all personnel with access to national intelligence have: a need for access, a favorable determination of eligibility made by an authorized adjudicative agency, and a signed non-disclosure agreement. These personnel shall be continually evaluated and monitored, and regularly trained in their individual security responsibilities. They shall also be advised of legal and administrative obligations and the ramifications of a failure to meet those obligations.

f. Establish CI and security awareness, training, and education programs that provide a common understanding and application of CI and security policies and standards.

g. Provide programmatic, budgetary, and other relevant information as requested by the NCIX, to support the NCIX's CI and security responsibilities as described in Section E.1.a.5 above.

h. Designate a Cognizant Security Authority (CSA) to serve as the IC element authority for all aspects of security program management for the protection of national intelligence and intelligence sources, methods, and activities. CSAs may formally delegate this responsibility to specific individuals within their elements.

**•Intelligence Community Directive 704 - Personnel Security Standards and Procedures**  
*Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*

-This directive applies to the IC, as defined by the National Security Act of 1947, as amended; and other departments or agencies that may be designated by the President, or designated jointly by the DNI, and the head of the department or agency concerned, as an element of the IC or those government entities designated to determine eligibility for SCI access.

-This Intelligence Community Directive establishes Director of National Intelligence (DNI) personnel security policy governing eligibility for access to Sensitive Compartmented Information (SCI) and information protected within other controlled access programs. This directive also documents the responsibility of the DNI for overseeing the program producing these eligibility determinations. It directs application of uniform personnel security standards and procedures to facilitate effective initial vetting, continuing personnel security evaluation, and reciprocity throughout the Intelligence Community (IC).

## **G. RESPONSIBILITIES**

-Heads of IC Elements are responsible for uniformly and consistently implementing DNI security policies governing access to classified national intelligence.

**•*Intelligence Community Directive 705 - Sensitive Compartmented Information Facilities***

-This ICD applies to the IC, as defined by the National Security Act of 1947, as amended, and other departments or agencies that may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the IC.

-This Directive establishes that all Intelligence Community (IC) Sensitive Compartmented Information Facilities (SCIF) shall comply with uniform IC physical and technical security requirements (hereinafter "uniform security requirements") . This Directive is designed to ensure the protection of Sensitive Compartmented Information (SCI) and foster efficient, consistent, and reciprocal use of SCIFs in the IC . This Directive applies to all facilities accredited by IC elements where SCI is processed, stored, used, or discussed .

## **Intelligence Community Standards**

**•*Intelligence Community Standard Number 700-2 – Use of Audit Data for Insider Threat Detection (Effective June 2, 2011)***

(Writer's note: As the text of this ICS is marked FOUO, go to [www.xxxxxx](http://www.xxxxxx) to access this document

## **Miscellaneous References**

Memorandum of Understanding (“MOU”): Reporting of Information Concerning Federal Crimes (signed by Intelligence Community agencies in 1995).

MOU between the FBI and EPA RE 811 Referrals, dated July 11, 2012.

U.S. Department of Justice, Office of Legal Counsel, MEMORANDUM OPINION FOR AN ASSOCIATE DEPUTY ATTORNEY GENERAL, “Legality of Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch,” August 14, 2009.

U.S. Department of Justice, Office of Legal Counsel, MEMORANDUM OPINION FOR THE COUNSEL TO THE PRESIDENT, “Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch,” January 9, 2009.

White House Memorandum, “Early Detection of Espionage and Other Intelligence Activities Through the Identification and Referral of Anomalies,” August 23, 1996.

Presidential Memorandum for the Heads of Executive Departments and Agencies, “National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs,” dated November 21, 2012.

U.S. Department of Justice Memorandum for the Attorney General from the Office of the Deputy Attorney General RE WARRANTLESS SEARCHES OF DOJ EMPLOYEES WITH ACCESS TO CLASSIFIED INFORMATION, October 15, 2001.

Office of Management and Budget (“OMB”) Circular No. A-130, Management of Federal Information Resources, Appendix III - Security of Federal Automated Information Resources.

MEMORANDUM FOR EXECUTIVE DEPARTMENTS AND AGENCIES from U.S. Office of Special Counsel, Special Counsel Carolyn N. Lerner, RE Agency Monitoring Policies and Confidential Whistleblower Disclosures to the Office of Special Counsel and to Inspectors General, dated June 20, 2012.

ATTORNEY GENERAL GUIDELINES FOR OFFICES OF INSPECTOR GENERAL WITH STATUTORY LAW ENFORCEMENT AUTHORITY, dated December 8, 2005.

Federal Register/Vol. 70, No. 29/Page 7513, Monday, February 14, 2005/Notices: Provides *Notice* concerning the routine uses of records maintained in the Federal Bureau of Investigation’s System of Records under the Privacy Act).

66 FR 33559, June 22, 2001, Blanket Routine Uses Applicable to More Than One FBI Privacy Act System of Records.



72 FR 3410, January 25, 2007, *DOJ Blanket Routine Use Authorizing Disclosure of Information in Response to a Data Breach*.

63 FR 8671, 8682, February 20, 1998, *Privacy Act System of Records Notice for the FBI Central Records System*.

MEMORANDUM FOR HEADS OF DEPARTMENTS AND AGENCIES, CHIEF HUMAN CAPITAL OFFICERS, AND AGENCY SECURITY OFFICERS, FROM: LINDA M. SPRINGER, DIRECTOR OF THE UNITED STATES OFFICE OF PERSONNEL MANAGEMENT, SUBJECT: Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide, January 14, 2008.

DoD Instruction O-5240.21, "Counterintelligence (CI) Inquiries," May 14, 2009.

(Writer's note: *See also*, DoD 5240 1-R, C2.3.2: "Publicly available information" about a U.S. person may be collected; and Executive Order 12333, section 2.3(a): Agencies within the Intelligence Community are authorized to collect, retain or disseminate information concerning United States persons that is publicly available or collected with the consent of the person concerned).

U.S. Department of Homeland Security, Privacy Impact Assessment for EINSTEIN 3 – Accelerated (E3A), April 19, 2013. (**Abstract:** The Department of Homeland Security (DHS), Office of Cybersecurity and Communications (CS&C) continues to improve its ability to defend federal civilian Executive Branch agency networks from cyber threats. Similar to EINSTEIN 1 and EINSTEIN 2, DHS will deploy EINSTEIN 3 Accelerated (E3A) to enhance cybersecurity analysis, situational awareness, and security response. With E3A, DHS will not only be able to detect malicious traffic targeting federal government networks, but also prevent malicious traffic from harming those networks. This will be accomplished through delivering intrusion prevention capabilities as a Managed Security Service provided by Internet Service Providers (ISP). Under the direction of DHS, ISPs will administer intrusion prevention and threat-based decision-making on network traffic entering and leaving participating federal civilian Executive Branch agency networks.

This Privacy Impact Assessment (PIA) is being conducted because E3A will include analysis of federal network traffic, which may contain personally identifiable information (PII).

## **Forms**

SF-75 (Request for Preliminary Employment Data)

SF-86 (EO10450 Questionnaire for National Security Positions);

SF 85 (Questionnaire for Nonsensitive Positions);

SF 85P (Questionnaire for Public Trust Positions);

SF-86A (Continuation Form for SF-86, SF-85, and SF-85P);

SF-312 (Classified Information Nondisclosure Agreement)

OF 306 (Declaration for Federal Employment);

OGE Forms 450, 278, 278T (Ethics Financial Disclosure Forms)

SF-713 (EO-12968 Consent to Access to Records);

Form 4414 (EF) (Sensitive Compartmented Information Nondisclosure Agreement);

FD-328 (Consent to Polygraph)

FD-857 (Sensitive Information Nondisclosure Agreement);

FD-868 (Nondisclosure Agreement for Joint Task Force Members, Contractors, Detailees, Assignees, and Interns);

FD-889 (IT Systems Use Agreement);

FD-979 (Personnel Consent to Release Information)

EO- 12564 (Drug-Free Federal Workplace) - (No specific federal forms. The testing requirement is found within specified "Position Descriptions" for pre-employment, random, and "for cause" employee drug screening)

DOJ-555 (Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act (Title 15, U.S. Code, Section 1681))