INTELLIGENCE COMMUNITY STANDARD NUMBER 700-1

GLOSSARY OF SECURITY TERMS, DEFINITIONS, AND ACRONYMS (EFFECTIVE DATE REMAINS: 4 APRIL 2008)

NOTICE: RENUMBERING OF INTELLIGENCE COMMUNITY STANDARD

A. REFERENCES: Intelligence Community Directive 101, *Intelligence Community Policy System* and Intelligence Community Policy Guidance 101.2, *Intelligence Community Standards*.

B. INTELLIGENCE COMMUNITY STANDARD (ICS) RENUMBERING: Per references, ICS 2008-700-1, *Glossary of Security Terms, Definitions, and Acronyms* is renumbered ICS 700-1. The content and page numbering of this ICS remain unchanged. This page is the coversheet for the existing ICS until its next revision.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
INTELLIGENCE COMMUNITY STANDARD
NUMBER 2008-700-1

SUBJECT: GLOSSARY OF SECURITY TERMS, DEFINITIONS, AND ACRONYMS

A. **AUTHORITY:** The National Security Act of 1947, as amended; the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004; Executive Order (EO) 12958, as amended; EO 12968; EO 12333, as amended; EO 13355, and other applicable provisions of law.

B. **APPLICABILITY:** The provisions of this Intelligence Community Standard (ICS) apply to the Intelligence Community (IC) as defined by the National Security Act of 1947, as amended; and other departments that may be designed by the President or designated jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned, as an element of the IC.

C. **SCOPE:** This ICS presents the DNI's approved security definitions and acronyms that apply to the 700 series Intelligence Community Directives (ICDs) and shall be used in all security documents promulgated by all IC security elements. This glossary relates only to security documents promulgated by IC security elements and does not apply to law enforcement activities such as electronic surveillance, forced entry, prosecutions for drug offenses, or espionage pursuant to Title 18.

D. **RESPONSIBILITIES:** All IC security elements shall ensure that the definitions and acronyms listed in the attached appendices are used within their respective programs. The DNI Special Security Center shall be responsible for all proposed amendments, additions, or deletions to this document.

E. **EFFECTIVE DATE:** This ICS becomes effective on the date of signature.

David R. Shedd
Deputy Director of National Intelligence
for Policy, Plans, and Requirements

April 4, 2008
Date

Appendix A

Glossary of Security Terms and Definitions

Terms	Definitions
Access	The ability or opportunity to obtain knowledge of classified or sensitive information.
Access Approval	Formal authorization for an individual to have access to classified or sensitive information within a Special Access Program (SAP) or a Controlled Access Program, including Sensitive Compartmented Information (SCI). Access requires formal indoctrination and execution of a non-disclosure agreement.
Access Control	A procedure to identify and/or admit personnel with proper security clearance and required access approval(s) to information or facilities using physical, electronic, and/or human controls.
Access Control System	A system of physical, electronic and/or human controls used to identify and/or admit authorized personnel to a facility or controlled area, e.g., Sensitive Compartmented Information Facility (SCIF) or internal compartmented area.
Access Eligibility Determination	A formal determination that a person meets the personnel security requirements for access to a specified type or types of classified information.
Accreditation	The formal certification by a cognizant security authority that a facility, designated area, or information system has met Director of National Intelligence (DNI) security standards for handling, processing, discussing, disseminating or storing Sensitive Compartmented Information.
Adjudication	Evaluation of personnel security investigations and other relevant information to determine if it is clearly consistent with the interests of national security for persons to be granted (or retain) eligibility for access to classified information, continue to hold sensitive positions, or continue to hold positions requiring a trustworthiness decision.
Adjudicative Process	An examination of a sufficient period of a person's life to make an affirmative determination that the person is an

	acceptable security risk.
Adjudicator	A personnel security specialist who performs adjudications.
Adverse Information	See: "Personnel Security – Issue Information."
Alien	Any person who is not a citizen of the United States (U.S.)
Appeal	A formal request under the provisions of Executive Order 12968, Section 5.2., for review of a denial or revocation of access eligibility.
Applicant	A person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information.
Authorized Adjudicative Agency	Any agency authorized by law, regulation, or direction of the Director of National Intelligence to determine eligibility for access to classified information in accordance with Executive Order 12968.
Authorized Classification and Control Markings Register	Also known as the "CAPCO Register," this is the official list of authorized security control markings and abbreviated forms of such markings for use by all elements of the Intelligence Community (IC) for classified and unclassified information.
Authorized Investigative Agency	Any agency authorized by law, executive order, regulation or the Director, Office of Management and Budget (OMB) under Executive Order 13381 to conduct counterintelligence investigations or investigations of persons who are proposed for access to sensitive or classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.
Background Investigation (BI)	An official inquiry into the activities of a person designed to develop information from a review of records, interviews of the subject, and interviews of people having knowledge of the subject.
Caveat	A designator used with or without a security classification to further limit the dissemination of restricted information, e.g., FOUO and NOFORN.
Certified TEMPEST Technical Authority (CTTA)	A U.S. Government employee who has met established certification requirements in accordance with the Committee on National Security Systems (CNSS)

	approved criteria and has been appointed by a U.S. Government department or agency to fulfill CTTA responsibilities.
Classification	An act or process by which information is determined to be classified.
Classification Guide	Guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.
Classification Levels	Information may be classified at one of the following three levels: *TOP SECRET*, which is applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe; *SECRET*, which is applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe; and *CONFIDENTIAL*, which is applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.
Classification Markings and Implementation Working Group	An IC forum comprised of IC and non-IC members that is responsible for coordinating changes to the Authorized Classification and Control Markings Register and associated implementation manual.
Classified National Security Information	Also known as "classified information." Any information that has been determined pursuant to Executive Order 12958, as amended; or any successor orders, to require protection against unauthorized disclosure and is marked to indicate its classified status.
Classifier	An individual who determines and applies a security classification to information or material. A classifier may be an original classification authority or a person who derivatively assigns a security classification based on a properly classified source or a classification guide.
Clearance	See: "Security Clearance."
Clearance Certification	An official notification that an individual holds a specific

	level of security clearance and/or access approval(s), authorizing the recipient of the certification access to classified information or materials at that level.
Cleared Escort	An appropriately cleared U.S. citizen, at least 18 years old, who performs access control/escort duties on limited and minor construction, repair or maintenance projects in Sensitive Compartmented Information Facilities or other classified areas that do not require a Construction Surveillance Technician.
Closed Storage	The storage of classified information in properly secured General Services Administration-approved security containers.
Coalition	An arrangement between one or more nations for common action; multi-national action outside the bounds of established alliances, usually for single occasions or longer cooperation in a narrow sector of common interest; or a force composed of military elements of nations that have formed a temporary alliance for some specific purpose.
Cognizant Security Authority (CSA)	The single principal designated by a Senior Official of the Intelligence Community (SOIC) to serve as the responsible official for all aspects of security program management concerning the protection of national intelligence, sources and methods, under SOIC responsibility.
Cohabitant	A person living in a spouse-like relationship with another person.
Collateral Information	National security information (including intelligence information), classified Top Secret, Secret, or Confidential that is not in the Sensitive Compartmented Information or other Special Access Program category.
Communications Security (COMSEC)	Measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. This includes crypto-security, transmission security, emission security, and physical security of communication security materials and information.
Compartmented Intelligence	National intelligence placed in a DNI-approved control system to ensure handling by specifically identified and access approved individuals.

Compelling Need	A signed determination by a Senior Official of the Intelligence Community, or his/her designee, that the services of an individual, based upon an assessment of risk, are deemed essential to operation or mission accomplishments.
Compromise	The disclosure or release of classified information to unauthorized person(s). See: "Unauthorized Disclosure."
Condition	See: "Personnel Security – Exception."
Confidential Source	Any individual or organization that provides information to the U.S. Government on matters pertaining to national security and expects, in return, that the information or relationship, or both, will be held in confidence. This definition is not to be confused with "intelligence source" as used in the Human Intelligence Community.
Construction Surveillance Technician (CST)	A citizen of the U.S., who is at least 18 years of age, cleared at the Top Secret level, experienced in construction and trained in accordance with the "Construction Surveillance Technician Field Guidebook" to ensure the security integrity of a site.
Continuous SCIF Operation	Staffing of a SCIF that is staffed and operated on a 24-hours a day, 7-days a week basis.
Contractor	Any industrial, educational, commercial, or other entity, grantee, licensee, and individual that has executed an agreement with the Federal Government for the purpose of performing under a contract, license, or other arrangements. This includes subcontractors of any tier, consultants, grantees, and cooperative agreement participants.
Contractor Special Security Officer (CSSO)	An individual appointed in writing by a cognizant security authority who is responsible for all aspects of SCI security at a U.S. Government contractor facility.
Controlled Access Programs	DNI-approved programs that protect national intelligence. They include: *Sensitive Compartmented Information* (SCI) compartments that protect national intelligence concerning or derived from intelligence sources, methods, or analytical processes; *Special Access Programs* (SAPs) pertaining to

	intelligence activities (including special activities, but excluding military operational, strategic and tactical programs) and intelligence sources and methods; and *Restricted collateral information*, other than SCI or SAPs, that imposes controls governing access to national intelligence or control procedures beyond those normally provided for access to Confidential, Secret, or Top Secret information, and for which funding is specifically identified.
Controlled Access Program Coordination Office (CAPCO)	The Director of National Intelligence's focal point for issues dealing with controlled access programs and support to the Controlled Access Program Oversight Committee and the Senior Review Group.
Controlled Access Program Oversight Committee (CAPOC)	The forum supporting the Director of National Intelligence in the management of controlled access programs. This includes the creation and continuation of controlled access programs including Sensitive Compartmented Information compartments and other Director of National Intelligence special access programs. It includes the monitoring of these programs through performance audits and evaluations as necessary.
Controlled Area	An area where physical entry is subject to restrictions for security purposes.
Corroborate	To strengthen, confirm, or make certain the substance of a statement through the use of an independent, but not necessarily authoritative source. For example, the date and place of birth recorded in an official personnel file that could be used to corroborate the date and place of birth claimed on a Standard Form 86. See: "Verify."
Counterintelligence (CI)	Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs.
Credit Check	Information provided by credit bureaus or other reporting services pertaining to the credit history of the subject of a personnel security investigation.

Custodian	Any person who has possession of, is charged with, or otherwise has been assigned responsibility for the control and accountability of classified information.
Damage Assessment	The analysis of the impact on national security of a disclosure of classified information to an unauthorized person.
Damage to the National Security	Harm to the national defense or foreign relations of the U.S. from unauthorized disclosure of information, taking into consideration such aspects as the sensitivity, value, utility and origin of that information.
Data	Information, regardless of its physical form or characteristics, that includes written documents, automated information systems storage media, maps, charts, paintings, drawings, films, photos, engravings, sketches, working notes, and papers, reproductions thereof by any means or process; and sound, voice, magnetic, or electronic recordings in any form.
Declassification	The authorized change in the status of information from classified to unclassified information.
Defense Central Index of Investigations (DCII)	An automated Department of Defense (DoD) repository that identifies investigations conducted by DoD investigative agencies. DCII does not contain eligibility information.
Defensive Travel Briefing	Formal advisories that alert travelers to the potential for harassment, exploitation, provocation, capture, entrapment, terrorism, or criminal activity. These briefings include recommended courses of action to mitigate adverse security and personal consequences and suggest passive and active measures to avoid becoming a target or inadvertent victim.
Denial	An adjudicative decision based on a personnel security investigation, other relevant information, or both, that an uncleared person is ineligible for access to classified information or special nuclear material. See: "Revocation."
Derivative Classification	Incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings of the source of the information.

	Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.
Derogatory Information	Issue information that adversely reflects on a person's loyalty, reliability and trustworthiness.
Designated Intelligence Disclosure Official (DIDO)	The heads of IC organizations or those U.S. Government Officials who have been designated by the DNI, in writing, as having the authority to approve or deny disclosure or release of uncaveated intelligence information to foreign governments in accordance with applicable disclosure policies and procedures.
Deviation	See: "Personnel Security – Exception."
Director of Central Intelligence Directive (DCID)	A directive issued by the Director of Central Intelligence that establishes general policies and procedures to be followed by intelligence agencies and organizations that were under his jurisdiction prior to the passage of the IRTPA. Note: Future Intelligence Community Directives, Intelligence Community Policy Memoranda and Intelligence Community Policy Guidance documents issued by the Director of National Intelligence will supersede all Director of Central Intelligence Directives.
Disclosure	Showing or revealing classified information, whether orally, in writing or any other medium, without providing the recipient material for retention. See "Release."
Dissemination	The provision of national intelligence to consumers in a form suitable for use.
Downgrading	A determination by the relevant classification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.
Dual Citizen	Any person who is simultaneously a citizen of more than one country.
Electronic Surveillance	Acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment

	solely to determine the location of the transmitter. Electronic surveillance may involve consensual interception of electronic communications and the use of tagging, tracking, and location devices. It should be noted that for the purpose of this glossary, this definition is general, and a more precise statutory definition may be found in Title 50 (Foreign Intelligence Surveillance Act).
Eligibility	See: "Access Eligibility Determination."
Emergency Action Plan (EAP)	A plan developed to prevent loss of national intelligence; protect personnel, facilities, and communications; and recover operations damaged by terrorist attack, natural disaster, or similar events.
Employee	For access determinations, 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.
Employee Assistance Program (EAP)	A program designed to provide counseling and referral services to employees having personal, alcohol, drug, financial, behavioral, or emotional problems.
Entrance National Agency Check (ENTNAC)	A personnel security investigation scoped and conducted on first-term enlistees into the military. This investigation type was discontinued in FY06 and has been replaced by the National Agency Check with Local Agency Checks and Credit Checks.
Espionage	(1) Intelligence activity directed toward the acquisition of information through clandestine means and proscribed by the laws of the country against which it is committed; or (2) Overt, covert, or clandestine activity designed to obtain information relating to the national security with intent or reason to believe that it will be used to the injury of the U.S. or to the advantage of a foreign nation. (See generally, The Espionage Act of 1917, 18 U.S.C., Sections 793, 794, and 798.)
Exception	See: "Personnel Security – Exception."

Expanded National Agency Check (ENAC)	Personnel security investigation requiring expansion of information developed from the National Agency Check.
Facility Accreditation	An official determination of the physical, procedural and technical security acceptability of a facility that authorizes its use to protect classified national security information.
Facility Certification	An official notification to the accreditor of the physical, procedural and technical security acceptability of a facility to protect classified national security information.
Facility Clearance	An administrative determination by the U.S. Government that a company is eligible for access to classified information or award of a classified contract.
Financial Crimes Enforcement Network (FINCEN)	An activity of the Department of the Treasury that supports law enforcement investigative efforts and fosters interagency and global cooperation against domestic and international financial crimes; it provides U.S. policymakers with strategic analyses of domestic and worldwide money laundering developments, trends, and patterns. FINCEN works toward those ends through information collection, analysis, and sharing, as well as technological assistance and implementation of the Bank Secrecy Act and other Department of Treasury authorities.
Financial Disclosure	A personnel security requirement for clearance processing that requires subjects to provide information regarding their total financial situation, e.g., assets, liabilities, and indebtedness.
Forced Entry	Entry by an unauthorized individual(s) that leaves evidence of the act.
Foreign Contact	Contact with any person or entity that is not a U.S. Person.
Foreign Government Information (FGI)	(1) Information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence; (2) information produced by the U.S. pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or (3) information received and treated as

	"foreign government information" under the terms of Executive Order 12958, as amended, or predecessor order.
Foreign Intelligence (FI)	Information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities.
Foreign National (FN)	Any person who is not a citizen of the U.S..
Foreign Ownership, Control or Influence (FOCI)	A U.S. company is considered under foreign ownership, control, or influence whenever a foreign interest has the power, direct or indirect, whether or not exercised and whether or not exercisable through ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information and/or special nuclear material or may affect adversely the performance of classified contracts.
Foreign Travel Briefing	A security briefing given to a person with access to classified information who intends to travel outside the U.S. See: "Defensive Travel Briefing."
Illegal Drug Use	The use of drugs, possession or distribution of which is unlawful under the Controlled Substances Act. Such term does not include the use of a drug taken under the supervision of a licensed health care professional, other uses authorized by the Controlled Substances Act or other provisions of law.
Immediate Family Member	For purposes of personnel security vetting, immediate family members include the spouse, parents, siblings, children, stepchildren and cohabitant of subject or applicant.
Incident of Security Concern	Events that, at the time of occurrence, cannot be determined to be an actual violation of law, but which are of such significance as to warrant preliminary inquiry and subsequent reporting. Examples include drug use and distribution, alcohol abuse, the discovery or possession of contraband articles in security areas, and unauthorized attempts to access classified data.
Indoctrination	Formal instruction to an individual approved for access to Sensitive Compartmented Information or Special Access

	Programs regarding program-unique information and program-specific security requirements and responsibilities.
Industrial Security	A multi-disciplinary security program concerned with the protection of classified information developed by or entrusted to U.S. industry.
Information Security (INFOSEC)	A system of administrative policies and procedures for identifying, controlling, and protecting, from unauthorized disclosure, information that is authorized protection by Executive Order or statute.
Information System(s) (IS)	Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.
Infraction	See: "Security Infraction"
Insider Threat	The ability of a trusted insider to bypass or defeat security safeguards or otherwise adversely affect the national security. See: "Internal Vulnerability."
Intelligence Activities	All activities that agencies within the IC are authorized to conduct pursuant to Executive Order 12333.
Intelligence Community Classification And Control Markings Implementation Manual	A companion document to the Authorized Classification and Control Marking Register (CAPCO Register) that provides guidance on the syntax and use of classification and control markings.
Intelligence Sources and Methods	(1) *Sources*: Persons, images, signals, documents, data bases, and communications media capable of providing intelligence information through collection and analysis programs, e.g., Human Intelligence, Imagery Intelligence, Signal Intelligence, Geospatial Intelligence and Measurement and Signature Intelligence; and (2) *Methods*: Information collection and analysis strategies, tactics, operations and technologies employed to produce intelligence products. If intelligence sources or methods are disclosed without authorization, their effectiveness may be substantially negated or impaired. (The term "intelligence sources and methods" is used in legislation and executive orders to denote specific protection responsibilities of the Director of National Intelligence.)

Interim Access Authorization (IAA)	A determination to grant access authorization prior to the receipt and adjudication of the individual's completed background investigation. See: "Temporary Access Eligibility."
Internal Vulnerability	The inside threat posed by an individual, with access to classified national intelligence, including Sensitive Compartmented Information, who may betray his or her trust. See: "Insider Threat:"
Issue Case	A case containing any issue information, even if fully mitigated.
Issue Information	See: "Personnel Security – Issue Information."
Intrusion Detection System (IDS)	A technical security system designed to detect an attempted or actual unauthorized entry into a secure facility or information systems and alert responders.
Joint Personnel Adjudication System (JPAS)	The centralized DoD database of standardized personnel security processes; virtually consolidates the DoD Central Adjudication Facilities by offering real time information concerning clearances, access, and investigative statuses to authorized DoD security personnel and other interfacing organizations (e.g., Defense Security Service, Defense Manpower Data Center, Defense Civilian Personnel Management System, Office of Personnel Management, and the Air Force Personnel Center).
Lead	Single investigative element of a case requiring action. Leads include reference interviews, record checks, subject interviews, local agency checks, and national agency checks.
Letter of Compelling Need	A written statement by a program manager or designee that the services of an individual with access eligibility issues, e.g., lacking U.S. citizenship or having foreign national family members, are essential to mission accomplishment.
Local Agency Check (LAC)	A review of the appropriate criminal history and court records in the jurisdictions over the areas where the Subject has resided, attended school, or been employed during a specific period of time.
Local Law Enforcement Check	See: "Local Agency Check."

Memorandum of Agreement (MOA)	A written agreement among relevant parties that specifies roles, responsibilities, terms, and conditions for each party to reach a common goal.
Minor Issue Information	See: "Personnel Security – Issue Information."
Mitigating Information	Personnel security information that tends to explain or refute factors that could otherwise support denial, revocation, or the granting of access only with an exception.
National Agency Check (NAC)	A personnel security investigation consisting of a review of: investigative and criminal history files of the Federal Bureau of Investigation, including a technical fingerprint check; Office of Personnel Management Security/ Suitability Investigations Index; Department of Defense Central Index of Investigations (DCII) and Joint Personnel Adjudication System (JPAS); and such other national agencies (e.g., Central Intelligence Agencey, Director of National Intelligence) as appropriate to the individual's background.
National Agency Check with Local Agency Checks and Credit Check (NACLC)	A personnel security investigation covering the immediately preceding five to seven years and consisting of a National Agency Check, financial review, verification of date and place of birth, and local agency checks.
National Intelligence	All intelligence, regardless of the source from which derived and including information gathered within or outside the U.S., that (A) pertains, as determined consistent with any guidance issued by the President, to more than one U.S. Government agency; and (B) that involves: *(i)* threats to the U.S., its people, property, or interests; *(ii)* the development, proliferation, or use of weapons of mass destruction; or *(iii)* any other matter bearing on U.S. national or homeland security.
National Security Information (NSI)	Any information that has been determined, pursuant to Executive Order 12958, as amended; or any predecessor order, to require protection against unauthorized disclosure and that is so designated.
Non-Disclosure Agreement (NDA)	An officially authorized contract between an individual and the U.S. Government signed by an individual as a condition of access to classified national intelligence. It specifies the security requirements for the access and details the penalties for noncompliance.

Non-Discussion Area	A defined area within a SCIF where classified discussions are not authorized.
Office of Management and Budget (OMB)	The U.S. Government element designated by Executive Order 13381 that is responsible for improving the process by which the government determines eligibility for access to classified national security information.
Office of Personnel Management (OPM)	The U.S. Government element responsible for the day-to-day supervision and monitoring of security clearance investigations and for tracking the results of individual agency-performed adjudications.
Open Storage	Storage of classified information within an approved facility not requiring use of General Services Administration-approved storage containers while the facility is not occupied by authorized personnel.
Operations Security (OPSEC)	A systematic and proven process intended to deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: (1) identification of critical information; (2) analysis of threats; (3) analysis of vulnerabilities; (4) assessment of risks; and (5) application of appropriate countermeasures.
Original Classification	An initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.
Original Classification Authority (OCA)	An individual authorized in writing, either by the President, the Vice President in the performance of executive duties, or by agency heads or other officials designated by the President, to classify information in the first instance
Periodic Reinvestigation (PR)	An investigation conducted at specified intervals, (i.e., 5 years or fewer for Top Secret access authorization, 10 years or fewer for Secret access authorization, and 15 years or fewer for Confidential access) to update a previously completed personnel security investigation.
Permanent Resident Alien	Any alien lawfully admitted into the U.S. under an immigration visa for permanent residence.

Personal Financial Statement	Form used as part of a personnel security investigation to provide a summary of a person's total monthly income, debt payments, expenses, and the net remainder of income.
Personnel Security	A security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information.
Personnel Security Exception	An adjudicative decision to grant or continue access eligibility despite a failure to meet all adjudicative or investigative standards. The head of the agency concerned or designee will make such decisions. (Exceptions with regard to eligibility for Sensitive Compartmented Information will be processed according to procedures established by the Director of National Intelligence.) For purposes of reciprocity, the presence of an exception permits the gaining organization or program to review the case before assuming security sponsorship and to accept or decline sponsorship based on that review. When accepting sponsorship, the gaining organization or program will ensure that the exception remains a matter of record. There are three types of exceptions: conditions, deviations, and waivers. (1) *Conditions:* Access eligibility granted or continued with the provision that additional security measures shall be required. Such measures include, but are not limited to, additional security monitoring, access restrictions, submission of periodic financial statements, and attendance at counseling sessions. (2) *Deviations*: Access eligibility granted or continued despite either a significant gap in coverage or scope in the investigation or an out-of-date investigation. "Significant gap" for this purpose means either complete lack of coverage for a period of six months or longer within the most recent five years investigated or the lack of an Federal Bureau of Investigations name check or technical check or the lack of one or more relevant investigative scope components (e.g., employment checks, financial review, or a subject interview) in its entirety. (3) *Waivers*: Access eligibility granted or continued despite the presence of substantial issue information that would normally preclude access. Agency heads or designees approve waivers only when the benefit of access clearly outweighs any security concern raised by

	the shortcoming. A waiver may require prescribed limitations on access such as additional security monitoring. See: "Personnel Security - Issue Information"
Personnel Security Interview	An interview conducted with an applicant for or holder of a security clearance to discuss areas of security relevance. The term is also used to describe interviews with references in personnel security investigations.
Personnel Security - Issue Information	Any information that could adversely affect a person's eligibility for classified information. There are two types of issue information: (1) *Minor Issue Information*: Information that meets a threshold of concern set out in "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," but for which adjudication determines that adequate mitigation, as provided by the Guidelines, exists. Minor issue information does not provide the basis for a waiver or condition. (2) *Substantial Issue Information*: Any information, or aggregate of information, that raises a significant question about the prudence of granting access eligibility. Substantial issue information constitutes the basis for granting access eligibility with waiver or condition, or for denying or revoking access eligibility.
Personnel Security Questionnaire (PSQ)	Security forms, whether paper or electronic, that are completed by a subject as part of a personnel security investigation. There are three versions of the PSQ: the Standard Form (SF) 85 for non-sensitive positions, the SF 85P for public trust positions, and the SF 86 for national security positions. See: "Questionnaire for National Security Positions."
Phased Periodic Reinvestigation (Phased PR)	A periodic reinvestigation which may exclude references and neighborhood check requirements when no information of security concern is developed through the other reinvestigation requirements.
Physical Security	The security discipline concerned with physical measures designed to: protect personnel; prevent unauthorized access to facilities, equipment, material, and documents; and defend against espionage, terrorism, sabotage, damage, and theft.

Physical Security Waiver	An exemption from specific standards for physical security for Sensitive Compartmented Information Facilities as outlined in Intelligence Community Directive 705.
Portable Electronic Devices (PEDs)	Electronic devices having the capability to store, record, and/or transmit text, images/video, or audio data. Examples of such devices include, but are not limited to: pagers, laptops, cellular telephones, radios, compact disc and cassette players/recorders, portable digital assistant, audio devices, watches with input capability, and reminder recorders.
Questionnaire for National Security Positions (QNSP)	The Standard Form 86 developed by the Office of Personnel Management for background investigations and reinvestigations. Completed by the applicant, the QNSP provides details on various aspects of the individual's personal and professional background.
Random Procurement	Method of acquiring, from existing local off-the-shelf stock, by Top Secret cleared U.S. citizens, materials for use in the new construction or modification to an existing SCIF or secure work area. Procurement of material will be unannounced, made without referral and immediately transported by the procurer to a Secure Storage Area. Random procurement may also be used for the acquisition of equipment, material, or supplies to be used in a SCIF or secure area.
Random Selection	The process of selecting a portion of building materials from bulk shipment procured for non-specific general construction use. Not authorized for SCIFs or Secure Work Areas.
Reciprocity	Recognition and acceptance, without further processing, of: (1) security background investigations and clearance eligibility determinations; (2) accreditations of information systems; and (3) facility accreditations. Reciprocity is obligatory in the IC when there are no waivers, conditions, or deviations to Director of National Intelligence security standards.
Reference	A person, other than the subject of a background investigation, identified as having knowledge of the subject. References are characterized by source and by type. There are two sources: *listed* (meaning the subject of the investigation identified the reference on the Personnel Security Questionnaire) and *developed*

	(meaning an investigator, in the course of pursuing leads, identified the reference as someone knowledgeable of subject). There are six types: *education* (a faculty member or school administrator at a school attended by the subject who had knowledge of the subject when a student), *employment/supervisor* (a person with management responsibilities for the subject), *co-worker* (a colleague with knowledge of the subject's on-the-job behavior), *neighborhood* (a person living in the subject's neighborhood who has knowledge of the subject), *friend/associate* (a person knowing the subject socially preferably away from both work and home), and other *knowledgeable person* (a person who knows the subject in some other context; for example: a banker or attorney or real estate agent who conducts business on behalf of the subject; or a clerk in a store where the subject shops frequently). A specific reference can be categorized as more than one type: for example, someone who is both an office mate and fellow member of a softball team may be both a co-worker reference and a friend/associate reference.
Release	Providing classified information in writing or any other medium for retention. See: "Disclosure."
Reinstatement	A process whereby an individual whose access authorization has been terminated or revoked is permitted to again have access to classified information.
Revocation	An adjudicative decision to permanently withdraw an individual's clearances based on a personnel security investigation, other relevant information, or both, that a cleared person is no longer eligible for access to classified information.
Risk	The probability of loss from an attack, or adverse incident. It is a function of threat (adversaries' capabilities, intentions and opportunities) and vulnerability (the inherent susceptibility to attack). Risk may be quantified and expressed in terms such as cost in loss of life, dollars, resources, programmatic impact, etc.
Risk Assessment	The process of evaluating security risks based on analyses of threats, vulnerabilities, and probable adverse consequences to a facility, system, or operation.
Risk Management	The process of selecting and implementing security countermeasures to accept or mitigate the risk of a known

	or suspected threat to an acceptable level based on cost and effectiveness. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.
Sabotage	The willful destruction of government property with the intent to cause injury, destruction, defective production of national defense, or war materials by either an act of commission or omission.
Safeguards	All measures taken to protect classified national intelligence, including Sensitive Compartmented Information from unauthorized disclosure.
Sanitization	The editing of intelligence to protect sources, methods, capabilities, and analytical procedures to permit wider dissemination.
Scattered Castles	The IC security clearance repository and the Director of National Intelligence's authoritative source for clearance and access information for all IC, military services, DoD civilians, and contractor personnel. DoD information is furnished by JPAS.
SCI Courier – (Certified)	Sensitive Compartmented Information (SCI) approved active duty military personnel, U.S. Government civilian employees, or contractor employees whose primary responsibility is to transport SCI material worldwide. The individual is so designated in writing and must have SCI access approvals at the level of material being transported.
SCI Courier–(Designated)	SCI approved active-duty military personnel, U.S. Government civilian employees, contractor employees or consultants whose temporary responsibility is to transport SCI material. The individual is so designated, in writing, and must have SCI access approvals at the level of material being transported.
SCIF Accreditation	Formal acceptance of a SCIF as meeting Director of National Intelligence security standards and formal authorization to process, store, and/or discuss SCI.
SCIF Co-utilization	The mutual agreement among two or more Government organizations to share the same SCIF.
SCIF Fixed Facility Checklist	A standardized document used in the process of certifying a SCIF. It documents all physical, technical, and procedural security information for the purpose of obtaining an initial or subsequent accreditation. Such information shall include, but not be limited to: floor

	plans, diagrams, drawings, photographs, details of electrical, communications, Heating, Ventilation and Air Conditioning connections, and security equipment layout. It shall also include any waiver information.
Scope	The time period to be covered and the sources of information to be contacted during the prescribed course of a personnel security investigation.
Secure Storage Area (Construction)	A room or area where materials intended for use in constructing a SCIF are securely stored pending the completion of the SCIF.
Secure Working Area (SWA)	An area accredited for handling, discussing and/or processing of classified information to include SCI, but not for the storage of such information.
Security Assurance	A written certification, from one government to another, of the security clearance level of their employees, contractors, and citizens. It includes an assurance by a responsible government security official that the proposed or intended recipient(s) of the classified information has the requisite security clearance and is authorized by the government to have access to classified information. It also includes an assurance that the recipient government will comply with any security requirements specified by the originating government. In the case of contractors, the security assurance must state the level of facility security clearance and, if applicable, the level of storage capability. The clearance information provided shall include the scope of the investigation upon which the clearance determination was based and the personal identity data of the individual.
Security Clearance	Also referred to as "clearance." An administrative authorization for access to national security information up to a stated classification level (Top Secret, Secret, or Confidential). A security clearance does not, by itself allow access to controlled access programs. See: "Access Approval," "Collateral Information," "Controlled Access Program," and "Special Access Program."
Security Countermeasures	Actions, devices, procedures, and/or techniques to reduce security risks.
Security Environment Threat List	A list of countries with U.S. Diplomatic Missions that is compiled by the Department of State and updated semi-annually. The listed countries are evaluated based on: transnational terrorism; indigenous terrorism; political

violence; human intelligence; technical threats; and criminal threats. The following four threat levels are based on these evaluations:

- *Critical* defined as a definite threat to U.S. assets based on adversary capability, intent to attack, and the targeting conducted on a recurring basis;

- *High* defined as a credible threat to U.S. assets based on knowledge of an adversary's capability, intent to attack, and related incidents at similar facilities;

- *Medium* defined as a potential threat to U.S. assets based on an adversary's desire to compromise the assets and the possibility that the adversary could obtain the capability to attack through a third party who has demonstrated such a capability; and

- *Low* defined as little or no threat as a result of the absence of credible evidence of capability, intent, or history of actual or planned attack against U.S. assets.

Security In-Depth	A concept of security calling for layered and complementary controls sufficient to detect and deter infiltration and exploitation of an organization, its information systems and facilities.
Security Incident	An act that constitutes a threat to a security program or is a deviation from existing governing security regulations. Security incidents may be portrayed as security infractions or security violations.
Security Infraction	A security incident involving a deviation from current governing security regulations that does not result in an unauthorized disclosure or compromise of national intelligence information nor otherwise constitutes a security violation.
Security Violation	A security incident involving: (1) any action that results in or could reasonably be expected to result in an unauthorized disclosure or compromise of classified information (including national intelligence); (2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of Executive Order 12958, as amended, or its implementing directives; or (3) any knowing, willful, or negligent action to create or continue a Special Access Program contrary to the requirements of Executive Order 12958, as amended.

Security/Suitability Investigations Index (SII)	The Office of Personnel Management database for personnel security investigations.
Self-Inspection	The internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under Executive Order 12958, as amended; and its implementing directives.
Senior Agency Official	The official designated by an agency head under section 5.4(d) of Executive Order 12958, as amended; to direct and administer the agency's program under which information is classified, safeguarded, and declassified.
Senior Foreign Official	Any foreign government official who, by virtue of his position or access, may directly affect his government's policy. These officials include, but are not limited to: those of ministerial rank and above; the heads of national departments, agencies and services; and representatives of ambassadorial rank and above.
Senior Intelligence Officer (SIO)	The highest-ranking military or civilian individual directly charged with foreign intelligence missions, functions, or responsibilities within a department, agency, component, command, or element of an IC organization.
Senior Official of the Intelligence Community (SOIC)	The head of an agency, organization, bureau, office, intelligence element or activities within the IC, as defined in Section 3 of the National Security Act of 1947, as amended, and Executive Order 12333.
Senior Review Group (SRG)	Provides advice and support to the Controlled Access Program Oversight Committee and serves as the managing body for compartmented programs under the purview of the Director of National Intelligence.
Sensitive But Unclassified Information	Protected unclassified information, the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or governmental interests.
Sensitive Compartmented Information (SCI)	Classified national intelligence concerning or derived from intelligence sources, methods, or analytical processes that is required to be protected within formal access control systems established and overseen by the Director of National Intelligence.

Sensitive Compartmented Information Facility (SCIF)	An area, room, group of rooms, buildings, or installation certified and accredited as meeting Director of National Intelligence security standards for the processing, storage, and/or discussion of SCI.
Sensitive Compartmented Information Facility Database	The IC database that provides a single source listing of Sensitive Compartmented Information Facilities worldwide and is used to promote continuity of operations and relocation of affected resources in the event of a national emergency.
Signal Flags	The IC database containing information used to assist security and counterintelligence professionals conducting National Agency Checks on individuals applying for positions with IC organizations.
Single Scope Background Investigation (SSBI)	A personnel security investigation consisting of all the elements prescribed in Standard B of ICPG 704.1, "Investigative Standards for Background Investigations for Access to Classified Information." The period of investigation for a SSBI varies, ranging from the immediately preceding 3 years for neighborhood checks to the immediately preceding 10 years for local agency checks.
Single Scope Background Investigation-Periodic Reinvestigation (SSBI-PR)	A periodic personnel security reinvestigation for Top Secret clearances and/or critical sensitive or special sensitive positions consisting of the elements prescribed in Standard C of ICPG 704.1, "Investigative Standards for Background Investigations for Access to Classified Information," initiated at any time following completion of, but not later than five years, from the date of the previous investigation or reinvestigation.
Site Security Manager (Construction)	A U.S. citizen, at least 18 years of age, cleared at the Top Secret level and approved for SCI, responsible for security where a SCIF is under construction.
Sound Masking System	An electronic system used to create background noise to mask conversations and counter audio-surveillance threats.
Special Access Program (SAP)	A program established for a specific class of classified

	information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.
Special Access Program Coordination Office (SAPCO)	The DoD focal point for issues pertaining to DoD controlled special access programs.
Special Access Program Oversight Committee (SAPOC)	Committee of DoD Under Secretaries that advises and assists the Secretary and Deputy Secretary of Defense in the management and oversight of DoD Special Access Programs.
Special Activities	Activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the U.S. Government is not apparent or acknowledged publicly, and functions in support of such activities, but which are not intended to influence U.S. political processes, public opinion, policies, or media and do not include diplomatic activities, the collection and production of intelligence, or related support functions.
Special Investigative Inquiry (SII)	A supplemental personnel security investigation of limited scope conducted to prove or disprove relevant allegations that have arisen concerning a person upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a personnel security determination.
Special Security Center (SSC)	The Director of National Intelligence element responsible for developing, coordinating, and overseeing Director of National Intelligence security policies and databases to support IC security elements. The SSC interacts with other IC security organizations to ensure that Director of National Intelligence equities are considered in the development of national level security policies and procedures.
Sponsoring Agency	A government department or agency that has granted access to classified national intelligence, including SCI, to a person whom it does not directly employ, e.g., a member of another government organization or a contractor employee.
Substantial Issue Information	See: "Personnel Security – Issue Information."

Tactical Approval to Operate (TAOP)	Cognizant Security Authority delegated authority to an operational element to allow a Tactical SCIF to be functional before formal accreditation is received. TAOP may not exceed one year in duration.
Tactical SCIF (T-SCIF)	An area, room, group of rooms, building, or installation accredited for SCI-level processing, storage and discussion, that is used for operational exigencies (actual or simulated) for a specified period of time not exceeding one year.
Tear Line	The place in an intelligence report (usually denoted by a series of dashes) at which the sanitized version of a more highly classified and/or controlled report begins. The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination, in accordance with the need-to-know, need-to-release, and write-to-release principles and foreign disclosure guidelines of the information below the tear line.
Technical Security	A security discipline dedicated to detecting, neutralizing, and/or exploiting a wide variety of hostile and foreign penetration technologies. The discipline mandates training in various countermeasure techniques.
Technical Surveillance Counter-Measures (TSCM)	Physical, electronic, and visual techniques used to detect and counter technical surveillance devices, technical security hazards, and related physical security deficiencies.
Technical Surveillance Counter-Measures Inspection	A government-sponsored comprehensive physical and electronic examination of an area by trained and specially equipped security personnel to detect or counter technical surveillance penetrations or hazards.
Technical Threat Analysis	A continual process of compiling and examining all available information concerning potential technical surveillance activities by intelligence collection groups which could target personnel, information, operations and resources.
TEMPEST	An unclassified term that refers to the investigation and study of compromising emanations.

Temporary Access Eligibility	Temporary eligibility for access that is based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements. (Constructed from the use of the term "temporary eligibility for access" in Executive Order 12968, Section 3.3.) See: "Interim Access Authorization."
Temporary Secure Working Area (TSWA)	A facility temporarily accredited to handle, process, or discuss classified information, to include SCI. The facility may not be used more than 40 hours per month and the accreditation may not exceed 6 months. SCI may not be stored in a TSWA.
Termination Security Briefing	A security briefing to remind individuals of their continued security responsibilities when their access authorization has been revoked, terminated, or suspended.
Threat	The intention and capability of an adversary to undertake actions that would be detrimental to the interests of the U.S.
Travel - Official	Travel performed at the direction of the U.S. Government.
Travel – Unofficial	Travel undertaken by an individual without official fiscal or other obligations on behalf of the U.S. Government.
Unauthorized Disclosure	A communication or physical transfer of classified national intelligence, including SCI, to an unauthorized recipient.
United States Citizen	A person born in the U.S. or any of its territories, a person born abroad but having one or both parents who are themselves U.S. citizens, and a person who has met the requirements for citizenship as determined by Immigration and Customs Enforcement and has taken the requisite oath of allegiance. The term "national of the U.S." must not be used synonymously with "U.S. citizen."
United States Person	A U.S. citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments.

Vault	An area constructed to afford maximum protection against forced entry that is used to store, handle, discuss, or process SCI.
Verify	To accept a statement as true based upon confirmation by an independent and authoritative source. For example, the birth certificate on file at the Bureau of Vital Statistics would be used to verify the date and place of birth claimed on an SF86. See: "Corroborate."
Waiver	See: "Personnel Security – Exception" and "Physical Security – Waiver."
Whole Person Concept	The basis upon which an access-granting authority makes an adjudicative determination of an individual's eligibility for access to classified information. This concept involves the careful weighing of all available information, favorable and unfavorable, both past and present, including mitigating factors.
Write-for-Release	Writing intelligence reports to disguise sources and methods to enable distribution to customers or intelligence partners at lower security levels. Write-to-release is proactive sanitization that makes intelligence more readily available to a more diverse set of customers.

Appendix B

Glossary of Security Abbreviations and Acronyms

AA	Accrediting Authority or Adjudication Authority
ACS	Access Control System
BI	Background Investigation
C & A	Certification & Accreditation
CAPCO	Controlled Access Program Coordination Office
CAPOC	Controlled Access Program Oversight Committee
CCTV	Closed Circuit Television
CD	Compact Disc
CI	Counterintelligence
CM	Countermeasures
CMIWG	Classification Markings Implementation Working Group
COMSEC	Communications Security
CSA	Cognizant Security Authority or Cognizant Security Agency
CSO	Cognizant Security Office
CSSO	Contractor Special Security Officer
CST	Construction Surveillance Technician
CTTA	Certified TEMPEST Technical Authority
DCID	Director of Central Intelligence Directive
DCII	Defense Central Index of Investigations
DIDO	Designated Intelligence Disclosure Official
EAP	Emergency Action Plan or Employee Assistance Program
ENAC	Expanded National Agency Check
ENTNAC	Entrance National Agency Check
EWG	Expert Working Group
FDF	Financial Disclosure Form
FFC	Fixed Facility Checklist
FGI	Foreign Government Information
FI	Foreign Intelligence

FINCEN	Financial Crimes Enforcement Network
FOCI	Foreign Ownership, Control or Influence
FRD	Formerly Restricted Data
IC	Intelligence Community
ICD	Intelligence Community Directive
ICPG	Intelligence Community Policy Guidance
ICPM	Intelligence Community Policy Memorandum
ID	Identification
IDS	Intrusion Detection System
IPMS	In Place Monitoring System
IRTPA	Intelligence Reform and Terrorism Prevention Act
IS	Information System
ISOO	Information Security Oversight Office
JPAS	Joint Personnel Adjudication System
LAC	Local Agency Check
MOA	Memorandum of Agreement
NAC	National Agency Check
NACLC	National Agency Check with Local Agency Checks and Credit Check
NCIX	National Counterintelligence Executive
NDA	Non-Disclosure Agreement
OCA	Originating Classification Authority
ODNI	Office of the Director National Intelligence
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPR	Office of Primary Responsibility
OPSEC	Operational Security
PAA	Principal Accrediting Authority
PCC	Policy Coordination Committee
PED	Portable Electronic Device
POC	Point of Contact
PSQ	Personal Security Questionnaire
SAO	Senior Agency Official

SAP	Special Access Program
SAPCO	Special Access Program Coordination Office
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SETL	Security Environment Threat List
SII	Security/Suitability Investigations Index or Special Investigative Inquiry
SIO	Senior Intelligence Officer
SISR	Signals Intelligence Security Regulations
SOIC	Senior Officials of the Intelligence Community
SOP	Standard Operating Procedure
SRG	Senior Review Group
SSBI	Single Scope Background Investigation
SSBI-PR	Single Scope Background Investigation-Periodic Reinvestigation
SSC	Special Security Center
SSCI	Senate Select Committee on Intelligence
SSM	Site Security Manager
SSO	Special Security Officer
SWA	Secure Working Area
TAOP	Tactical Approval To Operate
T-SCIF	Tactical-Sensitive Compartmented Information Facility
TSCM	Technical Surveillance Countermeasures
TSWA	Temporary Secure Working Area
TSWG	Technical Standards Working Group
UL	Underwriters Laboratories
VoIP	Voice over Internet Protocol

SUBJECT: GLOSSARY OF SECURITY TERMS, DEFINITIONS, AND ACRONYMS

Internal Distribution:

DDNI/PPR	CV MM
DDNI/A	SEC
DDNI/C	CFO
DDNI/AQ	SPP
OGC	SAE
ADNI S&T	CHCO
CIO	ADMIN
NCTC	E&T
NCPC	D/DIS
NCIX	DNI/SA
PM-ISE	DNI/XO
IRAN MM	EXEC SEC
NK MM	

External Distribution:

Director, Central Intelligence Agency
Director, Defense Intelligence Agency
Director, Office of Intelligence and Counterintelligence, Department of Energy
Assistant Secretary, Intelligence and Analysis, Department of Homeland Security
Assistant Secretary, Bureau of Intelligence and Research, Department of State
Assistant Secretary, Intelligence and Analysis, Department of Treasury
Chief of Intelligence/Senior Officer (SOIC), Drug Enforcement Administration
Executive Assistant Director, National Security Branch, Federal Bureau of Investigation
Director, National Geospatial-Intelligence Agency
Director, National Reconnaissance Office
Director, National Security Agency
Deputy Chief of Staff, G2 Army
Director of Naval Intelligence, United States Navy
Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance United States Air Force
Director of Intelligence, United States Marine Corps