GLOSSARY OF INTELLIGENCE TERMS AND DEFINITIONS

June 1989

PREFACE

This publication updates the 1978 *Glossary of Intelligence Terms and Definitions* that provided a baseline understanding of intelligence terms in a single document. The revision was developed by the Planning and Policy Office, Intelligence Community Staff, and reflects comments from the National Foreign Intelligence Council and the organizations that constitute the Intelligence Community.

The definitions in this revision of the Glossary have been devised by intelligence officers, not by philologists or semanticists. Thus, the terms and explanations contained herein are those that are commonly used and accepted by the Intelligence Community. Where some words may have several meanings within the intelligence context, a variety of definitions have been included. Where agencies or departments may have slightly different interpretations of a term, such definitions have been so indicated. Where useful, terms have been cross-referenced to convey contextual alternatives or to enhance its meaning by identifying its role within a larger concept (e.g., intelligence cycle). Section II, Acronyms and Abbreviations, contains items commonly seen or heard in the intelligence arena.

The Glossary does not include organizationally peculiar terms and definitions, highly specialized or technical vocabulary, or words or details that would require the document to be classified at a higher level. Some definitions may not coincide precisely with those used elsewhere for departmental or legal purposes, especially where they support and clarify the language of a legal document. Terms and acronyms that are not found in this Glossary may be found in other glossaries and publications listed in Section III.

The Glossary is designed to be a reference and guidance document for those who are new to the intelligence field, and to ease interdepartmental communications and understanding both within the Intelligence Community and with other governmental agencies. It is hoped that it will contribute to language commonality throughout the intelligence field. Users are encouraged to submit proposed corrections, additions, and suggestions to the Intelligence Community Staff, Planning and Policy Office, for incorporation in future updates of this Glossary. **Since this document represents a relatively comprehensive compilation and treatment of the intelligence terms that are used in implementing US foreign intelligence and counterintelligence activities, and the organizations involved, it should be treated and protected accordingly.**

CONTENTS

SECTION I
GLOSSARY

accreditation: (1) An official management authorization to operate an automated information system or network: a) in a particular security mode; b) with a prescribed set of administrative, environmental, and technical security safeguards; c) against a defined threat and with stated vulnerabilities and countermeasures; d) in a given operational environment; e) under a stated operational concept; f) with stated interconnections to other automated information systems or networks; and g) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility. (2) The acceptance by a foreign intelligence service official of the credentials of a US defense, military, naval, or air attache. (3) (DIA usage.) Acceptance of credentials by the Director, DIA, or a Service intelligence chief of a defense, military, naval, or air attache.

acoustical intelligence (ACINT): (1) Intelligence information derived from analysis of acoustic waves radiated either intentionally or unintentionally by the target into the surrounding medium. (2) In naval usage, the acronym ACINT usually refers to intelligence derived specifically from analysis of underwater acoustic waves from ships and submarines. (3) The technical and intelligence information derived from foreign sources that generate waves.

actionable intelligence: Intelligence information that is directly useful to customers for immediate exploitation without having to go through the full intelligence production process; it may address strategic or tactical needs, close support of US negotiating teams, or action elements dealing with such matters as international terrorism or narcotics.

active measures: A literal translation of a Russian phrase that is used to describe overt and covert techniques and intelligence operations designed to advance Soviet foreign policy objectives and to influence events in foreign countries by altering people's perceptions. Active measures should not be confused with legitimate diplomatic activities.

advisory tasking: A nondirective statement of intelligence interest or a request for intelligence information that is usually addressed by an element of the Intelligence Community to departments or agencies having information collection capabilities or intelligence assets not a part of the National Foreign Intelligence Program.

Advanced Imagery Requirements and Exploitation Systems (AIRES): A system operated by the DIA that provides automated support to DoD imagery analysts and collection managers and is the primary interface between DoD and national-level imagery requirements and exploitation systems.

agent: (1) A person who engages in clandestine intelligence activity under the direction of an intelligence organization but who is not an officer, employee, or co-opted worker of that organization. (2) An individual who acts under the direction of an intelligence agency or security service to obtain, or assist in obtaining, information for intelligence or counterintelligence purposes. (3) One who is authorized or instructed to obtain or to assist in obtaining information for intelligence or counterintelligence purposes.

agent authentication: The technical support task of providing an agent with personal documents, accouterments, and equipment that have the appearance of authenticity as to claimed origin and that support and are consistent with the agent's cover story.

agent of influence: (1) A person who is directed by an intelligence organization to use his position to influence public opinion or decisionmaking in a manner that will advance the objective of the country for which that organization operates. (2) An individual who can be used to covertly influence foreign officials, opinion molders, organizations, or pressure groups in a way that will generally advance US Government objectives, or to undertake specific action in support of US Government objectives.

agent net: An intelligence gathering unit of agents supervised by a principal agent who is operating under the direction of an intelligence officer. An agent net can be operative in either the legal or illegal field.

AIRES Life Extension (ALE): A program to maintain AIRES as a viable imagery support system into the 1990s. (Also see Advanced Imagery Requirements and Exploitation System.)

air-breathing missile: A missile with an engine requiring the intake of air for combustion of its fuel, as in a ramjet or turbojet. To be contrasted with the rocket missile, which carries its own oxidizer and can operate beyond the atmosphere.

air surveillance: (1) The systematic observation of air space by electronic, visual, or other means, primarily for the purpose of identifying and determining the movements of aircraft and missiles, friendly and unfriendly, in the air space under observation. (2) Any reconnaissance conducted by airborne platforms (i.e., aircraft, drones, balloons, satellites).

alert memorandum: A document issued by the DCI to National Security Council-level policymakers to warn them of possible developments abroad, often of a crisis nature, of major concern to the US; it is coordinated within the Intelligence Community to the extent time permits.

amplification: A request to NSA for information in greater detail on a given subject or event(s) than is stated in the Standing Requirement of the National SIGINT Requirements List. Such a request will normally be in effect for up to 90 days, but does not change the Standing Requirement or its priorities.

analysis: (1) A process in the production step of the intelligence cycle in which intelligence information is subjected to systematic examination in order to identify significant facts and derive conclusions therefrom. (Also see intelligence cycle.)

artificial intelligence: A computer science discipline concerned with building systems that exhibit the characteristics associated with intelligence in human behavior, e.g., understanding language, learning from experience, logical reasoning, solving problems, and explaining one's own behavior.

assessment: (1) Appraisal of the worth of an intelligence activity, source, information, or product in terms of its contribution to a specific goal, or the credibility, reliability, pertinency, accuracy, or usefulness of information in terms of an intelligence need. When used in contrast with evaluation assessment, implies a weighing against resource allocation, expenditure, or risk. (Also see evaluation.) (2) Judgment of the motives, qualifications, and characteristics of present or prospective employees or "agents." (Also see intelligence assessment and net assessment.)

asset: (1) Any resource—a person, group, relationship, instrument installation, supply—at the disposition of an intelligence agency for use in an operational or support role. (2) A person who contributes to a clandestine mission but is not a fully controlled agent. (Also see intelligence asset, national intelligence asset, and tactical intelligence asset.)

authentication: (1) A communications security measure designed to provide protection against fraudulent transmission and hostile imitative communications deception by establishing the validity of a transmission, message, station, or designator. (2) A means of identifying or verifying the eligibility of a station, originator, or individual to receive specific categories of information. (Also see communications deception.)

automated information system security: All of the technological safeguards and managerial procedures established and applied to computer hardware, software, and data in order to ensure the protection of organizational assets and individual privacy. This includes: all hardware/software functions, characteristics, and features; operational procedures; accountability procedures; access controls at all computer facilities; management constraints; physical protection; control of compromising emanations (TEMPEST); personnel and communication security; and other security disciplines.

Automated Tactical Target Graphic (ATTG): Format for broadly used target material that provides automated vertical or oblique photography of a target/installation and a limited portion of the surrounding area at a scale allowing maximum identification of target details. The accompanying text provides details concerning the physical characteristics of the target and its location.

background investigation: The means or procedures—such as selective investigations, record checks, personal interviews, and supervisory controls—designed to provide reasonable assurance that persons being considered for or granted access to classified information are loyal and trustworthy.

backstop: The arrangement made by documentary or oral means to support a cover story so that inquiries will elicit responses indicating the story is true.

basic intelligence: (1) Factual, fundamental, and generally permanent information about all aspects of a nation—physical, social, economic, political, biographical, and cultural—which is used as a base for intelligence products in support of planning, policymaking, and military operations. (2) General reference material for use in planning that pertains to the intentions, capabilities, vulnerabilities, and resources of other countries or potential operational theaters. (3) Intelligence, on any subject, that may be used as reference material for planning and in evaluating subsequent information. (Also see current intelligence, information, and intelligence.)

biographical intelligence: Foreign intelligence on the views, traits, habits, skills, importance, relationships, health, and curriculum vitae of those foreign personalities of actual or potential interest to the US Government.

bona fides: Documents, information, action, codes, etc., offered by an unknown or otherwise suspected individual in order to establish his good faith, identification, dependability, truthfulness, and motivation.

briefing: (1) Presentation, usually oral, of information. (2) Preparation of an individual for a specific operation by describing the situation to be encountered, the methods to be employed, and the objective.

brush contact: A discreet momentary contact, usually prearranged between intelligence personnel, during which material or oral information is passed.

cartographic intelligence: Intelligence primarily manifested in maps and charts of areas outside the United States and its territorial waters.

case officer: (1) A professional employee of an intelligence organization who is responsible for providing direction for an agent operation and/or handling assets. (Also see agent.)

CAUTION-PROPRIETARY INFORMATION INVOLVED (PROPIN): Warning designation used to identify information provided by a commercial firm or private source with the understanding that the information will be protected as a trade secret or proprietary data believed to have actual or potential value. Information bearing this marking shall not be disseminated in any form to an individual, organization, or foreign government that has any interest, actual or potential, in competition with the source of the information without the permission of the originator. This marking may be abbreviated as "PROPIN" or "PR."

Center: The headquarters site in the home country where control of intelligence and espionage operations in foreign countries is maintained.

Central Intelligence Agency (CIA): An Intelligence Community agency established under the National Security Council for the purpose of coordinating the intelligence activities of several US departments and agencies in the interest of national security. The CIA collects, produces, and disseminates foreign intelligence and counterintelligence; conducts counterintelligence activities abroad; collects, produces, and disseminates intelligence on foreign aspects of narcotics production and trafficking; conducts special activities approved by the President; and conducts research, development, and procurement of technical systems and devices.

Central Intelligence Agency Program (CIAP): See National Foreign Intelligence Program.

certification: The comprehensive evaluation of the technical and nontechnical security features of an automated information system or network, made as part of and in support of the accreditation process, that establishes the extent to which a particular design, its implementation, and its physical environment meet a specified set of security requirements.

cipher: (1) Any cryptographic system in which arbitrary symbols or groups of symbols represent units of plaintext. (2) A cryptographic system in which the cryptographic treatment (i.e., the method of transforming plaintext by predetermined rules to obscure or conceal its meaning) is applied to plaintext elements such as letters, digits, polygraphs, or bits that either have no intrinsic meaning or are treated without regard to their meaning in cases where the element is a natural-language word. (3) A method of concealing the meaning of a message either by replacing its letters with other letters or numbers in a predetermined manner (a substitution cipher) or by changing the order of the letters according to certain rules (a transportation cipher).

clandestine: Secret or hidden; conducted with secrecy by design.

clandestine collection: The acquisition of intelligence information in ways designed to assure the secrecy of the operation.

clandestine communication: Any type of communication or signal originated in support of clandestine operations. (Also see illicit communication.)

clandestine operation: A preplanned secret intelligence collection activity or covert political, economic, propaganda, or paramilitary action conducted so as to assure the secrecy of the operation; encompasses both clandestine collection and covert action.

Clandestine Service: That portion of the CIA that engages in clandestine operations; sometimes synonymous with the CIA Operations Directorate.

classification: The determination that official information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made; the designation is normally termed a *security classification* and includes: Confidential, Secret, and Top Secret. (Also see **declassification.**)

classification authority (derivative): An individual who assigns a classification to national security information based on criteria outlined in a classification guide, manual, or other authoritative document.

classification authority (original): The President, an agency head, or an individual delegated the authority (pursuant to Executive Order 12356) who makes an initial determination that certain information requires protection in the interest of national security, and who assigns a classification designator signifying the level of protection required.

classified information: (1) Official information that has been determined to require, in the interests of national security, protection against unauthorized disclosure and that has been so designated. (2) Information or material that is owned by, produced for, or under the control of, the US Government that has been determined by proper authority to require protection against unauthorized disclosure in the interest of national security and is so designated.

code: (1) A cryptographic system in which cryptographic equivalents (usually called *code groups*), typically consisting of letters and/or digits in otherwise meaningless combinations, are substituted for plaintext elements such as words, phrases, or sentences. (2) A system of communication in which arbitrary groups of symbols represent units of plaintext, used for brevity or security.

code word: (1) A word or term chosen to conceal the identity of a *function or action*, as distinguished from a *cover* name that conceals the identity of a person, organization, or installation. (2) A cryptonym used to identify sensitive intelligence data. (3) A word or term that conveys a prearranged meaning other than the conventional one; specifically, prearranged by the correspondents to increase security. (Also see **cover.**)

CODEWORD: Any of a series of designated words or terms used with a security classification to indicate that the material so classified was derived through a sensitive source or method, constitutes a particular type of sensitive compartmented information, and/or is otherwise accorded limited distribution.

collateral: All national security information classified under the provisions of an Executive Order for which special Intelligence Community systems of compartmentation (i.e., sensitive compartmented information) are not formally established.

collection: (1) The exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence. (2) Obtaining information or intelligence information in any manner, including direct observation, liaison with official agencies, or solicitation from official, unofficial, or public sources. (3) The act of employing instruments and/or equipment to obtain qualitative or quantitative data from the test or operation of foreign systems. (Also see **intelligence cycle.**)

collection guidance: See **guidance.**

collection plan: A plan for setting priorities and allocating resources to collect information from all available sources to meet intelligence requirements and for transforming those requirements into orders and requests to appropriate intelligence entities. (Also see **information, intelligence cycle.**)

collection requirement: (1) An established intelligence need considered in the allocation of intelligence resources to fulfill the essential elements of information and other intelligence needs. (2) An expression of an intelligence information need that requires collection and carries at least an implicit authorization to commit resources in acquiring the needed information. (3) A request for discipline-specific collection action to satisfy a specific or general intelligence information need. (Also see **intelligence requirement.**)

combat intelligence: Knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations. (Also see **tactical intelligence.**)

combined intelligence: (Military usage.) Intelligence produced by intelligence organizations of more than one country. (Also see **joint intelligence.**)

command, control, communications, and intelligence (C^3I): An integrated system of doctrine, procedures, organizational structure, personnel, equipment, facilities, communications, and supporting intelligence activities that provides authorities at all levels with timely and adequate data to plan, direct, and control their activities.

Committee on Imagery Requirements and Exploitation (COMIREX): A body within the Intelligence Community Staff responsible for advising and assisting the DCI in matters related to the collection, processing, and exploitation of imagery, and ensuring the effective use of Intelligence Community imagery collection and exploitation resources and products. (Refer to DCID 3/5.)

communications cover: See **manipulative communications cover.**

communications deception: The deliberate transmission, retransmission, alteration, absorption, or reflection of telecommunications in a manner intended to cause a misleading interpretation of these telecommunications. It includes: a) **imitative communications deception**—intrusion into foreign communications channels for the purpose of deception by introducing signals or traffic in imitation of the foreign communications and b) **manipulative communications deception**—the alteration or simulation of friendly telecommunications for the purpose of deception.

communications intelligence (COMINT): Technical and intelligence information derived from intercept of foreign communications by other than the intended recipients; it does not include the monitoring of foreign public media or the intercept of communications obtained during the course of counterintelligence investigations within the United States. COMINT includes the fields of traffic analysis, cryptanalysis, and direction finding.

communications security (COMSEC): (1) The protection resulting from all 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. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC equipment, material, and information. (2) Protective measures taken to deny unauthorized persons information of value that might be derived from telecommunications or to ensure the authenticity of such telecommunications. (3) The protection of US telecommunications and other communications from exploitation by foreign intelligence services and from unauthorized disclosure. (Also see **information systems security.**)

communications security signals acquisition and analysis: The acquisition of radiofrequency propagation and its subsequent analysis to determine empirically the vulnerability of the transmission media to interception by hostile intelligence services; it includes cataloging the transmission spectrum and taking signal parametric measurements as required, but does not include acquisition of information carried on the system; it is one of the techniques of communications security surveillance. (Also see **communications security surveillance.**)

communications security surveillance: The systematic examination of telecommunications and automatic data processing systems to determine the adequacy of communications security measures, to identify communications security deficiencies, to provide data from which to predict the effectiveness of proposed communications security measures, and to confirm the adequacy of such measures after implementation.

Community Counterintelligence and Security Countermeasures Office (CCISCMO): An office within the Intelligence Community Staff responsible for advising and assisting the DCI in assessing the foreign intelligence threat to the US and implementing counterintelligence and security countermeasures policy. (Refer to DCID 1/11.)

Community On-Line Intelligence System (COINS): A network of Intelligence Community computer-based information storage and retrieval systems that have been interconnected for interagency sharing of machine formatted files.

Compartmentation: (1) Formal system of restricted access to intelligence activities, such systems established by and/or managed under the cognizance of the DCI to protect the sensitive aspects of sources, methods, and analytical procedures of foreign intelligence programs. (2) The practice of establishing special channels for handling sensitive intelligence information, limited to individuals with a specific need for such information and who are therefore given special security clearances and indoctrination in order to have access to it. (3) Establishment and management of an intelligence

organization so that information about the personnel, organization, or activities of one component is made available to any other component or individual only to the extent required for the performance of assigned duties.

Compendium of Future Intelligence Requirements (COFIR): An Intelligence Community document listing future requirements for intelligence information, allowing for coordinated planning based on a common set of requirements.

compromise: (1) The exposure of classified official information or activities to persons not authorized access thereto; hence, unauthorized disclosure. (2) The known or suspected exposure of classified information or material in whole or in part to unauthorized persons through loss, theft, capture, recovery by salvage, defection of individuals, unauthorized viewing, or any other means. (3) The loss of control over any COMINT or information related to COMINT or COMINT activities resulting in a reasonable assumption that it could have, or confirmation of the fact that it has, come to the knowledge of an unauthorized person. (Also see **classified information.**)

compromising emanations: Unintentional emissions that could disclose information being transmitted, received, or handled by any information-processing equipment. (Also see TEMPEST.)

computer security (COMPUSEC): (1) The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized access, disclosure, acquisition, manipulation, modification, or loss of information in a computer system. (2) The computer-driven aspects of automated information system security encompassing the mechanisms and techniques that control access to or use of the computer or information stored in it. (3) The technical, administrative, and programmatic means by which assurance can be gained of correct, timely, and accountable delivery of appropriate information to authorized customers through automation. (Also see **automated information system security** and **information systems security.**)

CONFIDENTIAL: Security classification applied to information which, if disclosed in an unauthorized manner, could reasonably be expected to cause damage to national security.

Consolidated Cryptologic Program (CCP): See **National Foreign Intelligence Program.**

Consolidated Intelligence Resources Information System (CIRIS): The automated management information system used to identify and display the expected distribution of all intelligence resources within the National Foreign Intelligence Program.

consumer: An authorized person who uses intelligence or intelligence information directly in the decisionmaking process or to produce other intelligence; synonymous with customer and user.

co-opted worker: A national of a country, but not an officer or employee of the country's intelligence service, who assists that service on a temporary or regular basis. (In most circumstances a co-opted worker is an official of the country but might also be, for example, a tourist or student.)

Coordinating Committee for Multilateral Strategic Export Control (COCOM): A confidential multilateral organization that controls the export of strategic commodities and technology that could be used to strengthen the military potential of proscribed countries.

coordination: (1) The process of seeking concurrence from one or more groups, organizations, or agencies regarding a proposal or an activity for which they share some responsibility and that may result in contributions, concurrences, or dissents. (2) In intelligence production, the process by which producers gain the views of other producers on the adequacy of a specific draft assessment, estimate, or report; it is intended to increase a product's factual accuracy, clarify its judgments, and resolve or sharpen statements of disagreement on major contentious issues.

counterespionage: Aspect of counterintelligence designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities.

counterimagery: A subset of security countermeasures and operational security which is composed of measures taken to deny the undesirable imagery collection potential of both airborne and spaceborne platforms (e.g., camouflage).

counterinsurgency: Military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat insurgency.

counterintelligence: Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, persons, or terrorist activities, but not including personnel, physical, document, or communications security programs. (Also see **foreign counterintelligence, security countermeasures,** and **technical surveillance countermeasures.**)

countermeasures: See **security countermeasures** and **technical surveillance countermeasures.**

Countermeasures Advisory Panel (CAP): An interagency panel that recommends National TEMPEST policy for approval by the National Telecommunications and Information Systems Security Committee (NTISSC). (Also see TEMPEST.)

counterterrorism: Offensive measures taken to prevent, deter, and respond to a terrorist act, or the documented threat of such an act.

cover: Protective guise used by a person, organization, or installation to prevent identification with clandestine operations.

coverage: (1) The ground area represented on imagery, photomaps, mosaics, maps, and other geographical presentation systems. (2) The extent to which intelligence information is available in respect to any specified area of interest. (3) The summation of the geographical areas and volumes of aerospace under surveillance.

covert action: (1) An operation designed to influence governments, events, organizations, or persons in support of foreign policy in a manner that is not necessarily attributable to the sponsoring power; it may include political, economic, propaganda, or paramilitary activities. (2) Operations that are so planned and executed as to conceal the identity of, or permit plausible deniability by, the sponsor. (Also see **special activities.**)

covert communications: An assembly of clandestine communications equipment, techniques, and operational tradecraft used in the transmission of agent messages.

covert operation: See **clandestine operation** (preferred term). A covert operation encompasses covert action and clandestine collection.

critical intelligence: (1) Intelligence or information of such urgent importance to the security of the United States that it is directly transmitted at the highest priority to the President and other national decisionmaking officials before passing through regular evaluative channels. (2) Information concerning foreign events or situations that affect the national security interests of the United States to such an extent that it may require the immediate attention of the President and the National Security Council. (3) (Military usage.) Intelligence that requires the immediate attention of the commander to enable him to decide on a timely and appropriate response to potential/actual enemy actions. It includes, but is not limited to: a) strong indications of the imminent outbreak of hostilities of any type (warning of attack); b) aggression of any nature against a friendly country; c) indications or use of nuclear/biological chemical weapons (targets); and d) significant events within potential enemy countries that may lead to modification of nuclear strike plans.

Critical Intelligence Communications System (CRITICOMM): Those communications facilities under the operational and technical control of the Director, NSA, which have been allocated for the timely handling of critical intelligence. (Also see **critical intelligence.**)

cryptanalysis: The steps or processes involved in converting encrypted messages into plaintext without initial knowledge of the algorithm or key employed in the encryption.

CRYPTO: A designation that is applied to classified, cryptographic information that involves special rules for access and handling. (Also see **cryptographic information.**)

cryptographic information: All information significantly descriptive of cryptographic techniques and processes or of cryptographic systems and equipment, or their functions and capabilities, and all cryptomaterial. ("Significantly descriptive" means that the information could, if made known to unauthorized persons, permit recovery of specific cryptographic features of cryptoequipment, reveal weaknesses of associated equipment that could allow recovery of plaintext or of key, aid materially in the cryptanalysis of a general or specific crypto system, or lead to the cryptanalysis of an individual message, command, or authentication.) (Also see CRYPTO.)

cryptographic key: Information used to establish or change cryptoequipment for the purpose of encrypting or decrypting electronic signals.

cryptographic period: The time span during which a key setting for a crypto system remains in effect.

cryptographic security: The component of communications security that results from the provision of technically sound cryptographic systems and that provides for their proper use.

cryptographic system: All associated items of cryptomaterial (e.g., equipment and their removable components that perform cryptographic functions, operating instructions, and maintenance manuals) that are used as a unit to provide a single means of encryption and decryption of plaintext so that its meaning may be concealed; also any mechanical or electrical device or method used for the purpose of disguising, authenticating, or concealing the contents, significance, or meanings of communications; short name—**crypto system**.

cryptography: (1) The branch of cryptology used to provide a means of encryption and deception of plaintext so that its meaning may be concealed. (2) The enciphering of plaintext so that it will be unintelligible to an unauthorized recipient.

cryptologic activities: The activities and operations involved in the production of signals intelligence and the maintenance of signals security through cryptography and cryptographic principles.

cryptology: The science of producing signals intelligence and maintaining signals security. (Also see **cryptanalysis** and **cryptography**.)

cryptomaterial: (1) All material (including documents, devices, or equipment) that contains cryptographic information and is essential to the encryption, decryption, or authentication of telecommunications. (2) Communications Security (COMSEC) material bearing the marking CRYPTO or otherwise designated as incorporating cryptographic information. Cryptoequipments, their classified subdivisions, and keying material are considered cryptomaterial even though they do not bear the CRYPTO marking.

cryptosecurity: Shortened form of **cryptographic security**. See above.

crypto system: Shortened form of **cryptographic system**. See above.

current intelligence: (1) Intelligence of all types and forms of immediate interest to the users of intelligence; it may be disseminated without the delays incident to complete evaluation, interpretation, analysis, or integration. (2) Summaries and analyses of recent events.

damage assessment: (1) (Intelligence usage.) An evaluation of the impact of a compromise in terms of loss of intelligence information, sources, or methods, which may describe and/or recommend measures to minimize damage and prevent future compromises. (2) (Military usage.) An appraisal of the effects of an attack on one or more elements of a nation's strength (military, economic, and political) to determine residual capability for further military action in support of planning for recovery and reconstitution.

debriefing: Interviewing, under other than hostile conditions, of an individual who has completed an intelligence assignment or who has knowledge—through observation, participation, or otherwise—of operational or intelligence significance.

deception: Those measures designed to mislead a foreign power, organization, or person by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (Also see **communications deception**, **electronic countermeasures**, and **manipulative deception**.)

decipher: To convert an enciphered communication into its equivalent plaintext by means of a cipher system. (Also see **encipher** and **cipher**.)

declassification: Removal of official information from the protective status afforded by security classification; it requires a determination that disclosure no longer would be detrimental to national security. (Also see **classification**.)

decode: To convert an encoded message into its equivalent plaintext by use of a code. (Also see **encode** and **code**.)

decompartmentation: The removal of materials, information, or products from a compartmented system without altering them to conceal sources, methods, or analytical procedures. (Also see **compartmentation** and **sanitization**.)

decrypt: To transform an encoded or encrypted communication into its equivalent plaintext by means of a crypto system; this term includes the meanings of decipher and decode.

defection: Conscious (mental and/or physical) abandonment of loyalty, allegiance, duty, or principle to one's country.

defector: (1) A national of a designated country who has escaped from its control or who, being outside its jurisdiction and control, is unwilling to return and who is of special value to another

government because he is able to add valuable new or confirmatory intelligence information to existing knowledge about his country. (2) A person who, for political or other reasons, has repudiated his country and may be in possession of information of interest to the US Government. (Also see **emigre, refugee,** and **disaffected person.**)

Defense Intelligence Agency (DIA): An agency of the Intelligence Community responsible for satisfying the foreign military and military-related intelligence requirements of the Secretary of Defense, the Joint Chiefs of Staff, the Unified and Specified Commands, other Defense components, and, as appropriate, non-Defense agencies. It is a provider of military intelligence for national foreign intelligence and counterintelligence products, and is responsible for coordinating the intelligence activities of the military services and managing the Defense Attache System.

Defense Intelligence Community: Refers to the DIA, elements of the National Security Agency, and the intelligence offices of the Military Services, including the intelligence components of the Unified and Specified Commands, and DoD collectors of specialized intelligence through reconnaissance programs.

Defense Intelligence Officer (DIO): Senior officers who serve as principal substantive and operational intelligence advisers to the Director and Deputy Director, DIA, within their assigned geographic or functional area of responsibility. They represent the command element to intelligence users in the DoD, the Intelligence Community, executive departments and agencies, international organizations, and foreign governments.

Department of Defense Intelligence Information System (DODIIS): The aggregation of DoD personnel, procedures, equipment, computer programs, and supporting communications that support the timely and comprehensive preparation and presentation of intelligence and intelligence information to military commanders and national-level decisionmakers.

departmental intelligence: (1) Foreign intelligence produced and used within a governmental department or agency in support of its own activities and/or in meeting its assigned responsibilities. (2) Intelligence that any department or agency of the Federal Government requires to execute its own mission.

detection: A technical process wherein prescribed thresholds or specific conditions have been met and an expected indication of this condition is manifest. Examples: When a radio signal is strong enough to be displayed on a receiver; when an alarm system senses the movement of an intruder and sounds a bell. In general usage, the word *detection* implies both that the indication exists, and that it is recognized and properly interpreted.

direction finding (DF): A procedure for obtaining bearings on radiofrequency emitters with the use of a directional antenna and a display unit on an intercept receiver or ancillary equipment. Direction finding is a component of communications intelligence.

Director of Central Intelligence (DCI): (1) Primary adviser to the President and National Security Council on national foreign intelligence, appointed by the President with the consent of the Senate. (2) Head of the Intelligence Community and responsible for the development and execution of the National Foreign Intelligence Program. (3) Director of the Central Intelligence Agency.

Director of Central Intelligence Directive (DCID): A directive issued by the DCI that outlines general policies and procedures to be followed by intelligence agencies and organizations that are under his direction or overview.

Director of Central Intelligence Security Forum: A body composed of senior security managers from appropriate departments, agencies, and Intelligence Community organizations to support the DCI responsibilities assigned under the National Security Act of 1947 and relevant executive orders for the protection of both SCI and intelligence sources and methods. The forum develops and recommends to the DCI security policies, procedures, standards, and practices for the protection of SCI and intelligence sources and methods.

disaffected person: A person apparently disenchanted with his current situation who may therefore be exploitable for intelligence purposes; e.g., by the willingness to become an agent or defector. (Also see **walk-in.**)

disclosure: (1) The authorized release of classified information through approved channels. (2) The oral transmittal of information to an individual or individuals, or the visual exposure of tangible products such as images or textual/graphic materials; the disclosed products remain in US custody and control at all times. (Also see **release.**)

disinformation: Carefully contrived misinformation prepared by an intelligence service for the purpose of misleading, deluding, disrupting, or undermining confidence in individuals, organizations, or governments.

dissemination: The timely distribution of intelligence products (in oral, written, or graphic form) to departmental and agency intelligence consumers in a suitable form. (Also see intelligence cycle.)

DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR (ORCON): Security designation used to enable the originator of intelligence to control its wider distribution and use on a continuing basis. This marking is used on classified intelligence that clearly identifies or would reasonably permit ready identification of an intelligence source or method that is particularly susceptible to countermeasures that would nullify or measurably reduce its effectiveness. This marking may be abbreviated as "ORCON" or "OC."

document: In security terms, any recorded information, regardless of its physical form or characteristics, including: a) written or printed matter; b) automated data processing storage media containing recorded information; c) maps, charts, paintings, drawings, films, photos, engravings, sketches, working notes, and papers; and, d) sound, voice, magnetic, or electronic recordings of the above in any form.

documentation: Documents, personal effects, equipment, or anything supplied that will lend authenticity to intelligence personnel to support a cover story or legend.

domestic collection: The acquisition of foreign intelligence information within the United States from governmental or nongovernmental organizations or individuals who are witting sources and choose to cooperate by sharing such information.

double agent: An agent who is cooperating with an intelligence service of one government on behalf of and under the control of an intelligence or security service of another government, and is manipulated by one to the detriment of the other.

downgrade: To change a security classification from a higher to a lower level.

economic intelligence: (1) Intelligence regarding foreign economic resources, activities, and policies including the production, distribution, and consumption of goods and services, labor, finance, taxation, and other aspects of the international economic system. (2) (DIA usage.) The economic potential of a nation to wage war.

Economic Intelligence Committee (EIC): A body responsible for advising and assisting the DCI in the production of foreign economic intelligence and providing support to agencies charged with formulating US international economic policies. (Refer to DCID 3/12.)

electro-optical intelligence (ELECTRO-OPTINT): Intelligence information derived from the optical monitoring of the electromagnetic spectrum from ultraviolet (0.01 micrometers) through far (long wavelength) infrared (1,000 micrometers). (Also see optical intelligence.)

electronic countermeasures: Actions taken to prevent or reduce an adversary's effective use of the electromagnetic spectrum. (Also see electronic jamming and electronic deception.)

electronic counter-countermeasures: The division of electronic warfare involving actions taken to ensure the effective use of the electromagnetic spectrum despite an adversary's use of electronic countermeasures. (Also see electronic warfare.)

electronic deception: The deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in order to mislead or deny valid information to an enemy.

electronic emission security: Those measures taken to protect all transmissions from interception and electronic analysis.

electronic imagery dissemination: The transmission of imagery or imagery products by any electronic means. This includes the following four categories: a) *primary imagery dissemination system*—the equipment and procedures used in the electronic transmission and receipt of unexploited original or near-original-quality imagery in near-real time; b) *primary imagery dissemination*—the electronic transmission and receipt of unexploited original or near-original-quality imagery in near-real time through a primary imagery dissemination system. c) *secondary imagery dissemination*—the equipment and procedures used in the electronic transmission and receipt of exploited nonoriginal quality imagery and imagery products in other than real or near-real time; d) *secondary imagery dissemination*—the electronic transmission and receipt of exploited nonoriginal quality imagery and imagery products in other than real or near-real time through a secondary imagery dissemination system.

electronic intelligence (ELINT): (1) Technical and intelligence information derived from foreign electromagnetic noncommunications transmissions by other than the intended recipients. (2) Technical and intelligence information derived from foreign noncommunications electromagnetic radiations emanating from other than atomic detonation or radioactive sources.

electronic jamming: The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of disrupting an entity's use of electronic devices, equipment, or systems. (Also see **jamming.**)

electronic security (ELSEC): (1) The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their intercept and analysis of noncommunications electromagnetic radiations; e.g., radar. (2) The detection, identification, evaluation, and location of foreign electromagnetic radiations.

electronic surveillance: (1) Acquisition of a nonpublic communication by electronic means without the consent of at least one of the parties to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present within audible range of the communication. This does not include the use of radio direction-finding equipment solely to determine the location of a transmitter. (2) Surveillance conducted on a person, group, or other entity by electronic equipment.

electronic warfare (EW): Military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum, and action that retains friendly use of the electromagnetic spectrum. Electronic warfare consists of electronic warfare support measures, electronic countermeasures, and electronic counter-countermeasures.

electronic warfare support measures: That division of electronic warfare involving actions taken under direct control of an operational commander to search for, intercept, identify, and locate sources of radiated electromagnetic energy for the purpose of immediate threat recognition and tactical employment of forces. Data resulting from these measures can be used to produce SIGINT.

emanations security: The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from other than cryptographic equipment and telecommunications systems. (Also see **emission security.**)

Emergency Dissemination Authority: The DCI-delegated authority to disseminate, decompartment, or downgrade products that would facilitate US military operations or those of allied forces during a military emergency.

emigre: A person who departs from his country for any lawful reason with the intention of permanently resettling elsewhere. (Also see **refugee** and **defector.**)

emission control (EMCON): (1) The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security, detection by enemy sensors. (2) To minimize mutual interference among friendly systems.

emission security: The component of communications security resulting from all measures taken to deny to unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from cryptographic equipment and telecommunications systems. (Also see **emanations security.**)

encode: To convert plaintext into unintelligible form by means of a code. (Also see **code.**)

encipher: To convert a plaintext message into unintelligible form by the use of a cipher system. (Also see **cipher.**)

encrypt: To convert plaintext into an unintelligible form by means of a crypto system; this term includes the meanings of encipher and encode.

end product: See **finished intelligence.** (Also see **product.**)

energy intelligence: Intelligence relating to the technical, economic, and political capabilities and programs of foreign countries to engage in development, utilization, and commerce of basic and advanced energy technologies. This includes: the location and extent of foreign energy resources and their allocation; foreign government energy policies, plans, and programs; new and improved foreign energy technologies; economic and security aspects of foreign energy supply, demand, production, distribution, and utilization.

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. (2) Overt, covert, or clandestine activity designed to obtain information relating to the national defense with intent or reason to believe that it will be used to the injury of the United States or to the advantage of a foreign nation. For espionage crimes see Chapter 37 of Title 18, United States Code.

essential elements of information (EEIs): (1) Items of intelligence information essential for timely decisions and for enhancement of operations that relate to foreign powers, forces, targets, or the physical environments. (2) Targets (documents, instruments, etc.) that intelligence and/or security services attempt to obtain. (3) (Military usage.) The critical items of information regarding the enemy and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision.

estimate: (1) An analysis of a foreign situation, development, or trend that identifies its major elements, interprets the significance, and appraises the future possibilities and the prospective results of the various actions that might be taken. (2) An appraisal of the capabilities, vulnerabilities, and potential courses of action of a foreign nation or combination of nations in consequence of a specific national plan, policy, decision, or contemplated course of action. (3) An analysis of an actual or contemplated clandestine operation in relation to the situation in which it is or would be conducted in order to identify and appraise such factors as available and needed assets, and potential obstacles, accomplishments, and consequences. (Also see **intelligence estimate.**)

estimative intelligence: A category of intelligence that attempts to project probable future foreign courses of action and developments and their implications for US interests; it may or may not be coordinated and may be either national or departmental intelligence.

evaluation: (1) Appraisal of the worth of an intelligence activity, information, or product in terms of its contribution to a specific goal. (2) An appraisal of the credibility, reliability, pertinency, accuracy, or usefulness of information in terms of an intelligence need. Information is appraised at several stages within the intelligence cycle with progressively different contexts. Evaluation may be used without reference to cost or risk, particularly when contrasted with *assessment*. (3) A process in the production step of the intelligence cycle. (Also see **assessment, intelligence cycle.**)

evasion and escape (E&E): The procedures and operations whereby military personnel and other selected individuals are enabled to emerge from enemy-held or hostile areas to areas under friendly control.

evasion and escape intelligence: Processed intelligence information prepared to assist personnel to avoid capture if lost in enemy-dominated territory or to escape if captured.

exploitation: (1) The process of obtaining intelligence information from any source and taking advantage of it for intelligence purposes. (2) In SIGINT, the production of information from messages that are encrypted in systems whose basic elements are known. Exploitation includes decryption, translation, and the solution of specific controls such as indicators and specific keys. (Also see **source.**)

false flag recruitment: An individual recruited believing he/she is cooperating with an intelligence service of a specific country when, in reality, the individual has been deceived and is working on behalf of an intelligence service of another country.

feed material: Information, usually true but relatively unimportant, given to an individual to pass for the purpose of maintaining or increasing his/her value to another intelligence service. By increasing the individual's value, eventual passage of deceptive material and/or the obtaining of valued intelligence information is enhanced. Also called **developmental, passable,** or **build-up material.**

field review: A review of all security features associated with a system in its operational environment to ensure that minimum policy requirements are addressed. A field review is performed as part of the accreditation process.

finding: A determination made by the President stating that a particular intelligence operation is important to the national security of the United States, in compliance with the Foreign Assistance Act of 1961, as amended by the 1971 Hughes-Ryan Amendment.

finished intelligence: (1) The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. (2) The final result of the production step of the intelligence cycle; the intelligence product. (Also see **intelligence cycle** and **end product.**)

forecasting: Prediction, in the customary sense of assessing the magnitude a quantity will assume at some future point in time. Distinct from estimation that attempts to assess the magnitude of an already existing quantity.

foreign affairs community: Those US Government departments, agencies, and other organizations that are represented in US diplomatic missions abroad, and those that may not be represented abroad but are significantly involved in international activities with the governments of other nations.

foreign counterintelligence (FCI): Intelligence activity, with its resultant product, intended to detect, counteract, and/or prevent espionage and other clandestine intelligence activities, sabotage, international terrorist activities, or assassinations conducted for or on behalf of foreign powers, organizations, or persons; it does not include personnel, physical, document, or communications security programs. (Also see counterintelligence.)

Foreign Denial and Deception Analysis Committee (FDDAC): A committee that supports the DCI in the analysis of foreign activities to thwart US intelligence capabilities through denial and deception. (Refer to DCID 3/16.)

foreign instrumentation signals (FIS): Electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems that may have either military or civilian application; it includes but is not limited to, the signals from telemetry, beaconry, electronic interrogators, tracking/fusing/arming/command systems, and video data links.

foreign instrumentation signals intelligence (FISINT): Technical and intelligence information derived from intercept of foreign instrumentation signals (see above).

foreign integrated officer: An officer of a foreign government who occupies a position requiring access to US intelligence information in a host US agency and functions essentially as any other US personnel in the host agency.

foreign intelligence: (1) The product resulting from collection, evaluation, analysis, integration, and interpretation of intelligence information about a foreign power that is significant to the national security, foreign relations, or economic interests of the United States, provided by a government agency that is assigned an intelligence mission (i.e., an intelligence agency). (2) Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons (positive intelligence), but not including counterintelligence (with the exception of information on international terrorist activities). (3) Information relating to the ability of the United States to protect itself against actual or potential attack by, or other hostile acts of, a foreign power or its agents, or against the activities of foreign intelligence services. (Also see intelligence cycle.)

Foreign Intelligence Priorities Committee (FIPC): An Intelligence Community advisory committee responsible for developing, coordinating, monitoring, and updating the *Foreign Intelligence Requirements Categories and Priorities* document. (Refer to DCID 1/2.)

Foreign Intelligence Requirements Categories and Priorities (FIRCAP): A document that assigns priorities to requirements categories and foreign countries in a geotopical matrix and provides the Intelligence Community with basic substantive priorities guidance for the conduct of all US foreign intelligence activities. The priorities and requirements categories are revised and reissued on a current basis, and the entire document reissued on an annual basis. Formerly referred to as DCID 1/2 Attachment. (Also see priority.)

foreign intelligence service: An organization of a foreign government that engages in intelligence activities.

Foreign Language Committee (FLC): A DCI advisory committee that serves as the focal point for all matters dealing with recruitment, training, and retention of personnel with requisite foreign language expertise to serve the needs of the Community. (Refer to DCID 3/15.)

foreign liaison officer: A foreign official accredited by his government to one or more US departments or agencies to represent that government in the exchange and/or discussion of intelligence. The officer is authorized the same level of access as the country he represents and will be denied access to products that are not authorized for disclosure or release to that particular country. (Also see foreign integrated officer.)

foreign materiel (FORMAT or FM) intelligence: Intelligence derived from information gained by exploiting foreign equipment, subsystems, components, or other materiel.

foreign official: A person acting in an official capacity on behalf of a foreign power, attached to a foreign diplomatic establishment or an establishment under the control of a foreign power, or employed by a public international organization.

forward-looking infrared (FLIR) system: An infrared imaging system that uses a raster scan to view a scene by internal means, both horizontally and vertically. It can be spaceborne, airborne, seaborne, mounted on a ground vehicle, or placed at a fixed site. Its field of view is determined by the optics used, the scanning mechanism, and the dimensions of the detector array. **fusion**: (1) The blending of intelligence information from multiple sources to produce a single intelligence product. (2) (Military usage.) Integration of information to form a more comprehensive view of the tactical/theater/strategic situation, including the integration of intelligence information and operations data to form a clearer picture of the evolving battle.

fusion center: A term used within the DoD referring to an organization having the responsibility of blending both compartmented intelligence information with all other available information in order to support military operations. (Also see **actionable intelligence** and **tactical intelligence**.)

General Defense Intelligence Program (GDIP): See **National Foreign Intelligence Program**.

geographic(al) intelligence: Foreign intelligence dealing with the location, description, and analysis of physical and cultural factors of the world, (e.g., terrain, climate, natural resources, transportation, boundaries, population distribution) and their changes through time.

general medical intelligence (GMI): See **medical intelligence**.

guidance: (1) Advice that identifies, interprets, clarifies, and/or expands upon an information need. (2) The general direction of an intelligence effort, particularly in the area of collection. (Also see **human-source reporting**.)

high-frequency (HF) direction finding: Line of bearing determination, position fixing, and reporting of source locations of high frequency emissions as necessary to satisfy both national and tactical commanders' requirements.

House Permanent Select Committee on Intelligence (HPSCI): A permanent select committee of the House of Representatives established by House Rule XLVIII, whose function is to monitor and provide oversight over the Intelligence Community and intelligence-related activities of all other government organizations; the committee is also responsible for legislation pertaining to intelligence agencies and activities, including authorizing appropriations for such activities.

human intelligence (HUMINT): Intelligence information acquired by human sources through covert and overt collection techniques and open-source data from foreign media. (Also see **human-source reporting** and **human source**.)

human source: A person who wittingly or unwittingly conveys by any means information of potential intelligence value.

human-source reporting: (1) Intelligence information derived from human sources; it may come from information-gathering activities either within or outside the Intelligence Community. (2) An item of information being conveyed, as in human-source report. (Also see **human intelligence**.)

Human Resources Committee: A DCI advisory body, supported by the Intelligence Community Staff, responsible for assisting the DCI in the discharge of his responsibilities for the efficient allocation and effective use of Community resources for the collection of positive foreign intelligence information derived from human resources. (Refer to DCID 3/7.)

HUMINT Committee: See **Human Resources Committee**.

illegal: An officer or employee of an intelligence organization who is dispatched abroad and who has no overt connection with the intelligence organization with which he is connected or with the government operating that intelligence organization.

illegal agent: An agent operated by an illegal residency or directly by the headquarters of an intelligence organization. (Also see **illegal residency**.)

illegal communication: (1) An electronic communication or signal made without the legal sanction of the nation where it originates. (2) An electronic communication or signal originated in support of clandestine operations.

illegal residency: An intelligence apparatus, established in a foreign country and composed of one or more intelligence officers, which has no apparent connection with the sponsoring intelligence organization or with the government of the country operating the intelligence organization. (Also see **legal residency**.)

imagery: Representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media.

imagery collection products: The results of imagery intelligence collection when in the form of primary raw data. These data may be imagery and nonimagery materials, and include the primary image record and imagery technical data.

imagery-derived information: Intelligence products derived from imagery in other than photographic form. Examples of imagery-derived information are: textual reports, tables, graphic material (e.g., line drawings/artist concepts), automated data bases, cables, and oral information.

imagery intelligence (IMINT): The products of imagery and photographic interpretation processed for intelligence use. (Also see **imagery interpretation** below.)

imagery interpretation (II): The process of locating, recognizing, identifying, and describing objects, activities, and terrain represented on imagery; it includes *photographic interpretation*.

imagery products: Image reproductions derived from a primary image record that are in less than full frame format at contact or modified scale, and without titling and marginal data. Examples of imagery products are photographic prints, viewgraphs, transparencies, and digital image data.

imagery reconnaissance materials: Data associated with imagery reconnaissance—i.e., collection, intelligence, and map products—as well as imagery technical data. The term "material" is all inclusive and applies to such formats as briefings, target materials, memorandums, reports, and other publications associated with imagery reconnaissance.

imitative deception: The introduction of electromagnetic radiations into foreign channels that imitate that party's own emissions.

implant: An electronic device or component modification to electronic equipment that is designed to gain unauthorized interception of information-bearing energy via technical means.

indications: Information in various degrees of evaluation, all of which bears on the intention of a potential enemy to adopt or reject a course of action.

indications and warning (I&W): Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to US or Allied military, political, or economic interests, or to US citizens abroad. It encompasses forewarning of: enemy hostile actions or intentions; the imminence of hostilities; serious insurgency; nuclear/nonnuclear attack on the US, its overseas forces, or Allied nations; hostile reactions to US reconnaissance activities; terrorist attacks; and other similar events.

indicator: (1) An event, observation, or value used to measure an abstract concept. (2) An item of information that reflects the intention or capability of a potential enemy to adopt or reject a course of action. (3) An action—specific, generalized, or theoretical—that an enemy might be expected to take in preparation for an aggressive act.

indicator list: A list of the factors or acts (military, political, economic, diplomatic, and internal actions) a foreign power might be expected to take if it intended to initiate hostilities. These factors are logical/plausible moves derived from US reasoning, observations of past conflicts and crises, and intelligence assessments of enemy strategic offensive military doctrine and standard operating procedures.

infiltration: Placing an agent or other person in a target area in hostile territory, usually involving crossing a frontier or other guarded line. Methods of infiltration are black (clandestine), grey (through legal crossing point but under false documentation), or white (legal). May also include participation in an organization on an undisclosed basis.

informant: (1) A person who, wittingly or unwittingly, provides information to an agent, a clandestine service, or the police. (2) In reporting, a nonrecruited individual who has provided specific information and is cited as a source.

information: (1) Any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized data bases, paper, microform, or magnetic tape. (2) Unevaluated material of every description, at all levels of reliability, and from any source that may contain intelligence information. (Also see **intelligence information**.)

information handling: Management of data or information that may occur in connection with any step in the intelligence cycle; such management may involve activities to transform, manipulate, index code, categorize, store, select, disseminate, associate, or display intelligence materials; involve the use of printing, photographic, computer, or communications equipment, systems, or networks; it may include software programs to operate computers and process data and/or information; and may include information contained in reports, files, data bases, reference services, and libraries.

Information Handling Committee (IHC): A DCI advisory committee, supported by the Intelligence Community Staff, responsible for establishing common objectives for Intelligence Community information handling, and for coordinating the achievement of these objectives through improvement and integration of Intelligence Community information handling systems. (Refer to DCID 3/14.)

information need: The requirement of an official involved in the policymaking process or the intelligence production process for the best available information and intelligence on which to base policy decisions, recommendations, or intelligence production.

information security (INFOSEC): (1) The discipline covering the protection of classified National Security information by the application of the rules and procedures established by Executive Order 12356. It includes classification, declassification, marking, mandatory review, oversight, etc. (2) (Common usage.) The procedures pertaining to both **communications security** and computer security. (Also see **communications security** and **computer security**.)

information systems security: The protection afforded to information systems in order to preserve the availability, integrity, and confidentiality of the systems and information contained within the systems. Such protection is the application of the combination of all security disciplines that will, at a minimum, include COMSEC, TEMPEST, COMPUSEC, personnel security, industrial security, resource protection, and physical security.

infrared (IR): Electromagnetic radiation having wavelengths greater than visible light (0.75 millimeter) and shorter than microwaves (0.1 centimeter).

infrared imagery: A likeness or impression produced as a result of sensing electromagnetic radiations emitted or reflected from a given target surface in the infrared portion of the electromagnetic spectrum.

insurgency: An organized movement aimed at the overthrow of a constituted government through use of subversion and armed conflict.

integration: (1) A process in the production step of the intelligence cycle in which a pattern is formed the selection and combination of evaluatedligence information. (Also see **intelligence cycle**.) (2) In photography, a process by which the average radar picture seen on several scans of the time base may be obtained on a print, or the process by which several photographic images are combined into a single image.

intelligence: (1) A body of evidence and the conclusions drawn therefrom that is acquired and furnished in response to the known or perceived requirements of customers; it is often derived from information that is concealed or not intended to be available for use by the acquirer; it is the product of a cyclical process. (Also see **intelligence cycle**.) (2) A term used to refer collectively to the functions, activities, or organizations that are involved in the process of planning, gathering, and analyzing information of potential value to decisionmakers and to the production of intelligence as defined above. (3) The product resulting from the collection, collation, evaluation, analysis, integration, and interpretation of all collected information. (Also see **foreign intelligence** and **foreign counterintelligence**.)

intelligence activity: A generic term used to encompass any or all of the efforts and endeavors undertaken by intelligence organizations, including activities pursuant to collection, analysis, production, dissemination, and covert or clandestine activities. (Also see **intelligence organization**.)

intelligence agency: A component organization of the Intelligence Community. (Also see **Intelligence Community**.)

intelligence assessment: A category of intelligence production that encompasses most analytical studies dealing with subjects of policy significance; it is thorough in its treatment of subject matter—as distinct from building-block papers, research projects, and reference aids—but unlike estimative intelligence need not attempt to project future

developments and their implications; it is usually coordinated within the producing organization but may not be coordinated with other intelligence agencies. (Also see **estimative intelligence.**)

intelligence asset: Any resource—person, group, instrument, installation, or technical system—at the disposal of an intelligence organization.

intelligence collector: A phrase sometimes used to refer to an individual, system, organization, or agency that engages in the collection step of the intelligence cycle. (Also see **intelligence cycle.**)

Intelligence Community (IC): The aggregate of the following executive branch organizations and agencies involved in intelligence activities: the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research of the Department of State; intelligence elements of the military services, the Federal Bureau of Investigation, the Department of the Treasury, and the Department of Energy; and staff elements of the Office of the Director of Central Intelligence.

Intelligence Community Staff (ICS): The organization that supports the DCI in the exercise of Intelligence Community responsibilities assigned by Executive Order of the President. These include the examination of critical cross-disciplinary intelligence problems, coordination of Community priorities and requirements, maintenance of Community planning mechanisms, and development of the National Foreign Intelligence Program budget.

intelligence consumer: See **consumer.**

intelligence cycle: The process by which information is acquired and converted into intelligence and made available to customers. There are usually five steps in the cycle:

- **planning and direction**—determination of intelligence requirements, preparation of a collection plan, issuance of orders and requests to information collection entities, and continuous checks on the productivity of collection entities.
- **collection**—acquisition of information or intelligence information and the provision of this to processing and/or production elements. (Also see **collection.**)
- **processing**—conversion of collected information and/or intelligence information into a form more suitable for the production of intelligence. (Also see **processing.**)
- **production**—conversion of information or intelligence information into finished intelligence through the integration, analysis, evaluation, and/or interpretation of all available data and the preparation of intelligence products in support of known or anticipated customer requirements. (Also see **production.**)
- **dissemination**—timely conveyance of intelligence in suitable form to customers.

intelligence estimate: (1) The product of estimative intelligence. (Also see **estimate.**) (2) (Military usage.) An appraisal of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the probable order of their adoption.

intelligence information: Information of potential intelligence value concerning the capabilities, intentions, and activities of any foreign power, organization, or associated personnel.

intelligence information report (IIR): (Military usage.) A product of the collection step of the intelligence cycle. (Also see **intelligence report.**)

intelligence officer: A professional employee of an intelligence organization engaged in intelligence activities.

intelligence organization: A generic term that refers to any organization engaged in intelligence activities; it may include either an intelligence agency or a foreign intelligence service, or both. (Also see **intelligence agency** and **foreign intelligence service.**)

Intelligence Oversight Board (IOB): A body consisting of three nongovernment members appointed by, and reporting directly to, the President with responsibility for investigating intelligence activities that may be in violation of the Constitution, laws of the United States, Executive Orders, or Presidential objectives; membership and duties are expressed in Executive Order No. 12334.

intelligence producer: A phrase usually used to refer to an organization or agency that participates in the production step of the intelligence cycle. (Also see **intelligence cycle.**)

Intelligence Producers Council (IPC): An advisory body, supported in part by the Intelligence Community Staff, that assists and advises: a) the DCI in discharging those duties and functions that relate to intelligence production; b) the Director, Intelligence Community Staff, in production-related matters; and c) the Intelligence Community production managers in improving the overall effectiveness of the production process and the quality of the intelligence product by providing a consultative forum to address issues of interagency concern. (Refer to DCID 3/3.) (Also see National Intelligence Topics.)

intelligence-related activities (IRA): Those activities specifically excluded from the National Foreign Intelligence Program which: a) respond to departmental or agency tasking for time-sensitive information on foreign activities; b) respond to national Intelligence Community advisory tasking of collection capabilities that have a primary mission of supporting departmental or agency missions or operational forces; c) of training personnel for intelligence duties; or d) are devoted to research and development for intelligence and related capabilities.

intelligence report: (1) A product of the production step of the intelligence cycle. (Also see intelligence information report.) (2) (Military usage) A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. Also called INTREP.

intelligence reporting: The preparation and conveyance of information by any means. More commonly, the term is restricted to reports as they are prepared by the collector and as they are transmitted by him to his headquarters and by this component of the intelligence structure to one or more intelligence-producing components. Thus, reporting embraces both collection and dissemination.

intelligence requirement: Any subject, general or specific, upon which there is a need for the collection of intelligence information or the production of intelligence. (Also see collection requirement.)

Intelligence Research and Development Council (IR&DC): A senior body, supported by the Intelligence Community Staff, responsible for advising the DCI on research and development strategy and technologies that will best contribute to the attainment of national intelligence objectives. (Refer to DCID 3/4.)

intelligence user: See consumer.

Interagency Defector Committee (IDC): A committee that advises and assists the DCI in discharging his responsibilities with respect to the US Government Defector Program. (Refer to DCID 4/1.)

interagency intelligence memorandum (IIM): A national intelligence assessment or estimate issued by the DCI with the advice of appropriate National Foreign Intelligence Board components.

intercept(ion): Acquisition of electromagnetic signals (such as radio communications) by electronic collection equipment without the consent of the signalers for intelligence purposes.

international lines of communications: Those communications services under the supervision of the International Telecommunications Union and that carry paid public communications traffic between different countries; also known as International Civil Communications, International Commercial Communications, Internationally Leased Communications, International Service of Public Correspondence, and commercial communications.

International Telecommunications Satellite (INTELSAT): A global commercial communications satellite system owned and operated by members of the International Telecommunications Consortium.

international terrorism: Terrorist acts that transcend national boundaries in their conduct or purpose, the nationalities of the victims, or the resolution of the incident. Such an act is usually designed to attract wide publicity in order to focus attention on the existence, cause, or demands of the perpetrators.

international terrorist activity: The calculated use of violence, or the threat of violence, to attain political goals through fear, intimidation, or coercion; usually involves a criminal act, often symbolic in nature and intended to influence an audience beyond the immediate victims.

interpretability: Suitability of imagery for interpretation with respect to adequately answering requirements on a given type of target in terms of quality and scale.

interpretation: A process in the production step of the intelligence cycle in which the significance of information or intelligence information is weighed relative to the available body of knowledge. (Also see intelligence cycle.)

interrogation: Systematic effort to obtain information by direct questioning of a person under the control of the questioner.

intrusion detection systems (IDS): A security alarm system consisting of various types of components (balanced magnetic switches, capacitance, infrared, ultrasonic, etc.) to detect intrusion in the area of coverage within a facility.

jamming: See **electronic countermeasures.**

Joint Atomic Energy Intelligence Committee (JAEIC): An advisory committee responsible for advising and assisting the DCI in the area of production of national intelligence on foreign atomic energy issues. (Refer to DCID 3/9.)

joint intelligence: (1) (Intelligence usage.) Intelligence produced by intelligence organizations of more than one country. (2) (Military usage.) Intelligence produced by elements of more than one military service of the same nation. (Also see **combined intelligence.**)

Joint Intelligence Doctrine: DIA doctrine that establishes general guidelines for providing intelligence support to commanders of joint forces and enumerates principles for providing such support.

laser intelligence (LASINT): Technical and intelligence information derived from laser systems; it is a subcategory of electro-optical intelligence. (Also see **electro-optical intelligence.**)

legal residency: An intelligence apparatus in a foreign country composed of intelligence officers assigned as overt representatives of their government, but not necessarily identified as intelligence officers. (Also see illegal residency.)

line of sight: (1) The accessibility of a physical target in a direct and/or uninterrupted visual path to a distant surveillance point. (2) In communications, the need for the antenna of the receiving equipment to have a direct/unobstructed path to the transmitting antenna.

low-intensity conflict (LIC): A political-military confrontation between states or groups below the level of conventional war and above the routine, peaceful competition among states. Involving protracted struggles of competing principles and ideologies, it is waged by a combination of political, economic, informational, and military instruments.

manipulative communications cover: Those measures taken to alter or conceal the characteristics of communications so as to deny to any enemy or potential enemy the means to identify them. Also known as *communications cover.*

manipulative communications deception: See **communications deception.**

manipulative deception: The alteration or simulation of friendly electromagnetic radiations to accomplish deception.

mapping, charting, and geodesy products: Graphic or statistical representation of the Earth's characteristics as follows: a) at an established scale, of natural or artificial features on the surface or a part or the whole of the earth or other planetary body. The features are positions relative to a coordinate reference system; b) *chart*—a special purpose map, generally designed for navigation or other particular purposes, in which essential map information is combined with other data critical to the intended use (e.g., aeronautical chart, hydrographic chart); c) *geodesy*—the science of determining the size and shape of the Earth, which determines the external gravitational field of the Earth and three dimensional points on, above, and below the Earth's surface.

measurement and signature intelligence (MASINT): Scientific and technical intelligence information obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the source, emitter, or sender and to facilitate subsequent identification and/or measurement of the same.

Measurement and Signature Intelligence (MASINT) Committee: A body, supported by the Intelligence Community Staff, established to advise and assist the DCI with respect to the collection, processing, and reporting of measurement and signature intelligence. (Refer to DCID 3/17.)

medical intelligence (MEDINT): (1) Medical scientific, technical, and biological intelligence that assesses and predicts technological advances of medical significance, to include defense against chemical, biological, and radiological warfare; it

applies to both tactical and strategic planning and operations, including military and humanitarian efforts. (2) Intelligence related to all aspects of foreign natural and manmade environments that could influence the health of military forces. (3) Assessments of foreign medical capabilities in both military and civilian sectors. (Also see biographical intelligence.)

military intelligence (MI): Intelligence on any foreign military or military-related situation or activity that is significant to military policy making or the planning and conduct of military operations and activities.

Military Intelligence Board (MIB): A policy and decisionmaking body chaired by the Director, DIA, and composed of the four military service intelligence chiefs. The board meets periodically to establish guidance and to coordinate intelligence issues affecting the services and DIA in their support of the DoD and the Intelligence Community.

monitor: To continuously observe a person or event, or to observe, hear, intercept, record, or transcribe any form of communication or media, for collection of intelligence information or communications security purposes, either overtly or covertly.

monitoring: An intelligence function involving the collection, analysis, and reporting of information on activities of another party related to arms control agreements. Monitoring contributes to the verification process by providing assessments used by policymaking officials in determining compliance or noncompliance with arms control agreements.

multilevel security: (For automated information systems.) (1) Provisions for the safeguarding of all information within a multilevel information handling system that permit various levels and/or compartments of data to be concurrently stored and processed in an automated information system but ensuring that only personnel with the appropriate security clearances have access to selected information. (2) A security yardstick that is attained when some users of an information system do not have a national intelligence clearance for access to some of the information in the system—also called *multilevel mode of operation.* (Also see unilevel security.)

national estimate: See national intelligence estimate.

National Foreign Intelligence Board (NFIB): The senior Intelligence Community advisory body to the DCI on the substantive aspects of national intelligence. This Board advises the DCI on: production, review, and coordination of national foreign intelligence; interagency exchanges of foreign intelligence information; arrangements with foreign governments on intelligence matters; the protection of intelligence sources and methods; activities of common concern; and such other matters as are referred to it by the DCI. It is composed of the DCI (Chairman), and other appropriate officers of the Central Intelligence Agency, Department of State, Department of Defense, Department of the Treasury, Department of Energy, the Defense Intelligence Agency, the National Security Agency, the Federal Bureau of Investigation and, as necessary, the offices within the Department of Defense for reconnaissance programs. Senior intelligence officers of the Army, Navy, Marine Corps, and Air Force participate as observers, as does a representative of the Assistant to the President for National Security Affairs. (Refer to DCID 3/1.)

National Foreign Intelligence Council (NFIC): The senior Intelligence Community advisory body to the DCI on national intelligence issues, other than the substantive aspects that are the responsibility of the NFIB. The NFIC advises the DCI on priorities and objectives for the National Foreign Intelligence Program budget and matters that are referred to it by the DCI. Membership includes all agencies listed under National Foreign Intelligence Board, the Chairman of the Intelligence Producers Council, and representatives from the offices of the Attorney General, Secretary of Defense, and Secretary of Commerce. (Refer to DCID 3/2.)

National Foreign Intelligence Program (NFIP): Includes the following activities, though its composition is subject to review by the National Security Council and modification by the President: Central Intelligence Agency programs, the Consolidated Cryptologic Program, the General Defense Intelligence Program, and elements of programs of the offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance, other programs of agencies within the Intelligence Community designated jointly by the DCI and the head of the department or by the President as national foreign intelligence or counterintelligence activities, and activities of the staff elements of the DCI. Intelligence activities required for the planning and

multilateral treaty arrangements and organizations, and foreign political movements directed against or affecting established governments or authority.

positive intelligence: A term of convenience sometimes applied to foreign intelligence to distinguish it from foreign counterintelligence.

President's Foreign Intelligence Advisory Board (PFIAB): A body consisting of senior nongovernment members appointed by, and reporting directly to, the President, empowered to assess the quality, quantity, and adequacy of intelligence collection, of analysis and estimates, of counterintelligence, and other intelligence activities with a view toward increasing the effectiveness of the national intelligence effort; specific duties and responsibilities are outlined in Executive Order 12331.

primary imagery dissemination: See electronic imagery dissemination.

primary imagery dissemination system: See electronic imagery dissemination.

primary imaging record (PIR): The collection product associated with imaging reconnaissance, including the original negative, duplicate positives, and/or duplicate negatives when in original full-frame format with associated titling and marginal data.

principal agent: An agent who, under the direction of an intelligence officer, is responsible for the operational activities of other agents.

priority: A value denoting a preferential rating or precedence in position that is used to discriminate among competing entities; the term normally used in conjunction with intelligence requirements in order to illuminate importance and to guide the actions planned, being planned, or in use to respond to the requirements.

Priority Intelligence Requirements: Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decisionmaking. Formerly termed Essential Elements of Information.

processing: (1) The conversion of collected information and/or intelligence information into a form more suitable for the production of intelligence. (2) Further handling, manipulation, consolidation, composition, etc., of information to convert it from one format to another or to reduce it to manageable and/or intelligible information. (3) In photography, the operations necessary to produce negatives, diapositives, or prints from exposed films, plates, or paper. (Also see intelligence cycle.)

product: (1) An intelligence report disseminated to customers by an intelligence agency. (2) In SIGINT usage, intelligence information derived from analysis of SIGINT materials and published as a report or translation for dissemination to customers.

production: The preparation of reports based on analysis of information to meet the needs of intelligence users (consumers) within and outside the Intelligence Community. (Also see intelligence cycle.)

propaganda: Any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly.

proprietary: A business entity owned, in whole or in part, or controlled by an intelligence organization and operated to provide private commercial cover for an intelligence activity of that organization. (Also see cover.)

psychological operations (PSYOP): Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

radar intelligence (RADINT): Intelligence information derived from data collected by radar.

radiation intelligence (RINT): The functions and characteristics derived from information obtained from unintentional electromagnetic energy emanating from foreign devices; excludes nuclear detonations or radioactive sources.

raw intelligence: A colloquial term meaning collected intelligence information that has not yet been converted into finished intelligence. (Also see intelligence information.)

reconnaissance (RECCE or RECON): An operation undertaken to obtain, by visual observation or other detection methods, information relating to the activities, resources, or forces of a foreign

conduct of tactical operations by the United States military forces are not included in the National Foreign Intelligence Program. (Also see Tactical Intelligence and Related Activities.)

National HUMINT Collection Plan (NHCP): A document prepared by the HUMINT Committee providing the Intelligence Community with coordinated DCI HUMINT collection guidance, assessing the responsiveness of HUMINT reporting to national-level consumers, and recommending improvements in HUMINT collection and reporting.

National Imagery Interpretability Rating Scale (NIIRS): A graduated decimal scale standard, providing quality evaluation of optical imagery through an estimate of potential intelligence content. Used as a standard value by collection, exploitation, processing, production, and user personnel.

national intelligence: (1) Foreign intelligence produced under the aegis of the DCI and intended primarily to be responsive to the needs of the President, the National Security Council, and other Federal officials involved in the formulation and execution of national security, foreign, political, and/or economic policy. (2) Integrated departmental intelligence that covers the broad aspects of national policy and national security, is of concern to more than one department or agency, and transcends the exclusive competence of a single department or agency.

national intelligence asset: An intelligence asset funded in the National Foreign Intelligence Program, the primary purpose of which is the collection or processing of intelligence information or the production of national intelligence. (Also see intelligence asset and national intelligence.)

National Intelligence Council (NIC): The National Intelligence Council is comprised of the National Intelligence Officers (NIOs), their staff, and an analytic group. The NIOs support the DCI by producing national intelligence estimates, other interagency assessments, and by advising him on the intelligence needs of policymakers.

National Intelligence Daily (NID): A Community-produced digest of current intelligence drafted daily (six times a week) for use by senior government officials.

National Intelligence Estimate (NIE): (1) A thorough assessment of a situation in the foreign environment that is relevant to the formulation of foreign, economic, and national security policy, and that projects probable future courses of action and developments; it is structured to illuminate differences of view within the Intelligence Community; it is issued by the DCI with the advice of the National Foreign Intelligence Board. (2) A strategic estimate of capabilities, vulnerabilities, and probable courses of action of foreign nations that is produced at the national level as a composite of the views of the Intelligence Community. (Also see Special National Intelligence Estimate.)

National Intelligence Officer (NIO): The senior staff officer of the DCI for an assigned area of functional or geographic responsibility. The NIO manages estimative and interagency intelligence production on behalf of the DCI; he is the principal point of contact between the DCI and intelligence consumers below the cabinet level and is a primary source of national-level substantive guidance to Intelligence Community planners, collectors, and resource managers. (Also see National Intelligence Council.)

National Intelligence Topics (NITs): An annual document published by the Intelligence Producers Council representing the critical intelligence needs of senior US policymakers.

National Military Intelligence Center (NMIC): An indications and warning center that operates 24 hours a day, responsible for providing time-sensitive intelligence to the National Military Command Center, the Secretary of Defense, Joint Chiefs of Staff, the Unified and Specified Commands, and the Military Services.

National Radar Interpretability Scale (NRIS): A gaduated decimal scale standard, providing quality evaluation of radar imagery through an estimate of potential intelligence content. Used as a standard value by collection, exploitation, processing, production, and user personnel.

national security: The territorial integrity, sovereignty, and international freedom of action of the United States. *Intelligence activities relating to national security* encompass all the military, economic, political, scientific, technological, and other aspects of foreign developments that pose actual or potential threats to US national interests.

National Security Agency (NSA): An agency of the Intelligence Community responsible for centralized coordination, direction, and performance of highly specialized technical functions in support of

US Government activities to protect US communications and produce foreign intelligence information. It coordinates, directs, and performs all cryptologic functions for the US Government; collects, processes, and disseminates SIGINT information for DoD, national foreign intelligence, and counterintelligence purposes; and is the national executive agent for classified communications and computer security.

National Security Directive (NSD): A document that promulgates Presidential decisions implementing national policy and objectives in all areas involving national security. All decision directives are individually identified by number and signed by the President.

National SIGINT Requirements List (NSRL): A registry of all approved SIGINT requirements levied on the US SIGINT System.

National SIGINT Requirements System (NSRS): The process by which intelligence requirements flow from originators, through validation and acceptance by the Intelligence Community, to levy on the US SIGINT System (USSS) through the National SIGINT Requirements List, and ultimately, to the evaluation of the responsiveness of the USSS to these requirements.

National SIGINT Operations Center (NSOC): The principal 24-hour watch office responsible for current SIGINT production and for answering user agency queries.

national/tactical interface: A relationship between national and tactical intelligence activities encompassing the full range of fiscal, technical, operational, and programmatic matters.

National Telecommunications and Information Systems Security Committee (NTISSC): An interagency committee responsible for approving national security policies for safeguarding systems which process or communicate sensitive information.

near-real-time: The brief interval between the collection of information regarding an event and reception of the data at some other location, caused by the time required for processing, communications, and display.

"NEED-TO-KNOW": (1) The fundamental security principle in safeguarding classified information, which ensures that such information is accessible only to those persons with appropriate clearance, access approval, and a clearly identified need-to-know. (2) A criterion used in security procedures that requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform his official duties.

net assessment: A comparative review and analysis of opposing national strengths, capabilities, vulnerabilities, and weaknesses. An *intelligence net assessment* involves only foreign countries.

NOT RELEASABLE TO CONTRACTORS/ CONSULTANTS (NOCONTRACT): Security designation used to identify classified intelligence that may not be released to contractors or consultants without the permission of the originating agency. This marking is used on intelligence that is provided by a source on the condition that it not be made available to contractors, or on intelligence that would actually or potentially give a contractor a competitive advantage, and could reasonably be expected to cause a conflict of interest with the obligation to protect the information. This marking may be abbreviated as "NOCONTRACT" or "NC."

NOT RELEASABLE TO FOREIGN NATIONALS NOFORN): Security designation used to identify classified intelligence that may not be released in any form to foreign governments, foreign nationals, or non-US citizens without permission of the originator. This marking is used on intelligence that could jeopardize intelligence sources or methods or be detrimental to the best interests of the United States. This marking may be abbreviated "NOFORN" or "NF."

nuclear intelligence (NUCINT): Intelligence derived from the collection and analysis of radiation and other effects resulting from radioactive sources.

nuclear proliferation intelligence: Foreign intelligence relating to: a) scientific, technical, and economic capabilities, programs, political plans, and intentions of nonnuclear weapons states or organizations to acquire nuclear weapons and/or to carry on research, development, and manufacture of nuclear explosive devices; and b) the attitudes, policies, and actions of foreign nuclear supplier countries or organizations toward provision of technologies, facilities, or special nuclear materials that could assist nonnuclear weapon states or organizations to acquire or develop nuclear explosive devices.

official: See foreign official.

official information: Information that is owned by, produced for or by, or is subject to, the control of the US Government.

open-source information: Information of potential intelligence value (i.e., intelligence information) available to the general public such as papers, books, periodicals, and other printed information. It also includes information derived from radio and television transmissions, press agencies, publications, maps, and photography.

operational electronic intelligence (OPELINT): The category of electronic intelligence concerned with the introduction, disposition, movement, utilization, tactics, and activity levels of known foreign noncommunications emitters and, where applicable, associated military systems.

operational intelligence (OPINTEL): (1) Intelligence required for planning and executing operations. (2) Intelligence required for planning and executing all types of military operations.

operations security (OPSEC): A systematic and analytic process by which the US Government can deny potential adversaries information about its capabilities and intentions by identifying, controlling, and protecting evidence of the planning and execution of sensitive activities and operations.

optical intelligence (OPTINT): That portion of electro-optical intelligence that deals with visible light. (Also see **electro-optical intelligence.**)

order of battle (OB): Intelligence pertaining to identification, strength, command structure, and disposition of the personnel, units, and equipment of any foreign military force. (Also see **technical intelligence.**)

overt: Open; done without attempt at concealment.

overt collection: The acquisition of intelligence information from public media, observation, government-to-government dialogue, elicitation, and from the sharing of data openly acquired; the process may be classified or unclassified; the target and host governments as well as the sources involved normally are aware of the general collection activity although the specific acquisition, sites, and processes may be successfully concealed.

Peacetime Reconnaissance and Certain Sensitive Programs (PRCSO): Procedures for conducting reconnaissance under the control of the Joint Chiefs of Staff. Formerly known as Peacetime Aerial Reconnaissance Program (PARPRO).

penetration: (1) The recruitment of agents within or the infiltration of agents or introduction of technical monitoring devices into an organization or group or physical facility for the purpose of acquiring information or influencing its activities. (2) In automatic data processing operations, the unauthorized extraction and identification of recognizable information from a protected ADP system.

persona non grata (PNG): An official act of declaring a foreign national as being unacceptable or unwelcome in a country. This term usually applies to situations where the Department of State declares an official foreign representative persona non grata when they have been detected engaging in intelligence activities or otherwise violating US law.

personnel security: The means or procedure—such as selective investigations, record checks, personal interviews, and supervisory control—designed to provide reasonable assurance that persons being considered for or granted access to classified information are loyal and trustworthy.

photographic intelligence (PHOTINT): See **imagery intelligence.**

photographic interpretation (PI): See **imagery interpretation.**

physical security: (1) The component of security that results from all physical measures necessary to safeguard classified equipment and material from access by unauthorized persons. (2) Physical measures—such as safes, vaults, perimeter barriers, guard systems, alarms and access control—designed to safeguard installations against damage, disruption, or unauthorized entry; information or material against unauthorized access or theft; and specified personnel against harm.

plaintext: (1) Normal text or language, or any symbol or signal that conveys information without any hidden or secret meaning. (2) Unencrypted communications; specifically, the original message of a cryptogram, expressed in ordinary language.

planning and direction: See **intelligence cycle.**

platform: In collection parlance, the conveyance for technical collection sensors.

political intelligence: Intelligence concerning the dynamics of the internal and external political affairs of foreign countries, regional groupings,

nation; or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.

recruitment: Process of enlisting an individual to work for an intelligence or counterintelligence service.

recruitment-in-place: A person who agrees to become an agent and retain his position in his organization or government while reporting on it to an intelligence or security organization of a foreign country.

RED/BLACK Concept: The separation of electrical and electronic circuits, components, equipment, and systems that handle classified plain-language information in electric signal form (RED) from those that handle encrypted or unclassified information (BLACK); RED and BLACK terminology is used to clarify specific criteria relating to and differentiating between such circuits, components, equipment, and systems and the areas in which they are contained.

redoubled agent: An agent whose dual role has been discovered by the service on which he is reporting and who is used, wittingly or unwittingly, voluntarily or under duress, to serve the purpose of the latter service against the former service.

referentura: Soviet term used to describe the suite of rooms that exist in Soviet diplomatic establishments abroad that are specially reinforced and swept for hostile eavesdropping devices.

refugee: A person outside the country or area of his former habitual residence who, because of fear of being persecuted or because of hostilities in that country or area, is unwilling or unable to return to it. (Also see **defector** and **emigre**.)

release: The physical transfer of a tangible intelligence product to an authorized recipient for retention who then assumes responsibility for the appropriate physical security of, and access to, such products. (Also see **disclosure**.)

report: See **intelligence report** and **intelligence information report**.

Request for Information (RFI): (1) A request by a consumer for information from another intelligence organization. Normally, an RFI is a one-time request for which a specific response is required and is terminated when the request is answered or by mutual agreement between the originator and the intelligence organization. (2) A request to the NSA by a consumer for information that is presumed to be available in NSA's existing holdings.

requirement: A general or specific request for intelligence information made by a member of the Intelligence Community. (Also see **intelligence requirement** or **collection requirement**.)

requirements category: A category of substantive foreign intelligence information that is of interest to the US Government. The DCI approves priorities for requirements categories that are reference points for intelligence cycle actions. (Refer to DCID 1/2.)

Requirements Management System (RMS): A joint DIA/CIA program to provide the national and DoD IMINT communities with a uniform collection requirements management system.

residency: See **legal residency** and **illegal residency**.

sabotage: Destruction or damage to material, premises, utilities, or their production for the purpose of impairing or weakening an organization, government, or nation.

safehaven: (1) A protected or reinforced area within an official facility or personal residence located overseas to which occupants can retreat during an emergency and remain until the situation returns to normal or outside help arrives. (2) A foreign country or a protected area within a foreign country affording a hiding place or temporary asylum for persons evading hostile government elements.

safehouse: A house or premises controlled by an intelligence organization that affords—at least temporarily—security for individuals involved or equipment used in clandestine operations.

sanitization: The process of editing or otherwise altering intelligence materials, information, reports, or other products to conceal and protect sensitive intelligence sources, methods, capabilities, analytical procedures, or privileged information in order to permit wider dissemination.

scientific and technical (S&T) intelligence: Intelligence concerning foreign developments in basic and applied scientific and technical research and development including engineering and production techniques, new technology, and weapon systems and their capabilities and characteristics; it also includes intelligence that requires scientific or

technical expertise on the part of the analyst, such as medicine, physical health studies, and behavioral analyses.

Scientific and Technical Intelligence Committee (STIC): An advisory committee responsible for advising and assisting the DCI with respect to the production, coordination, and evaluation of intelligence on foreign scientific and technical developments that could affect significantly the national security of the United States. (Refer to DCID 3/10.)

secondary imagery dissemination: See **electronic imagery dissemination.**

secondary imagery dissemination system: See **electronic imagery dissemination.**

SECRET: Security classification applied to information which, if disclosed in an unauthorized manner, could reasonably be expected to cause serious damage to national security.

security: Establishment and maintenance of protective measures that are intended to ensure a state of inviolability from hostile acts or influences.

TYPES OF SECURITY

Automatic Data Processing System Security
Communications Security
Computer Security
Cryptographic Security
Electronic Emission Security
Electronic Security
Emanation Security
Emission Security
Information Security
Multilevel Security
National Security
Operations Security
Personnel Security
Physical Security
Signals Security
Transmission Security
Unilevel Security

security classification: See **classification.**

security clearance: An administrative determination by a competent national authority that an individual is eligible, from a security standpoint, for access to classified information.

security countermeasures: Defensive security programs and activities that seek to protect against both foreign intelligence collection efforts and unauthorized access to, or disclosure of, protected facilities, information, and material.

security mode of operation of an automated information system: A security yardstick that indicates the relative level of risk to information in an automated information system. There are four modes of operation: dedicated, system high, compartmented, and multilevel. The mode of operation is defined as a comparison between information sensitivity and user trust.

security survey: A comprehensive formal evaluation of a facility, area, or activity by security specialists to determine its physical or technical strengths and weaknesses; and to propose recommendations for improvement.

Senate Select Committee on Intelligence (SSCI): A select committee of the Senate established by Senate Resolution 400 whose function is to monitor and provide oversight over the Intelligence Community and intelligence-related activities of all other government organizations; the Committee is also responsible for legislation pertaining to intelligence agencies and activities, including authorizing appropriations for such activities.

senior intelligence officer (SIO): The highest ranking military or civilian individual charged with direct foreign intelligence missions, functions, or responsibilities within a department, agency, component, command, or element of an Intelligence Community organization.

Senior Officials of the Intelligence Community (SOICs): The heads of the organizations comprising the Intelligence Community or their designated representatives.

sensitive: Requiring special protection from disclosure to avoid compromise or threat to the security of the sponsor.

sensitive compartmented information facility (SCIF): An accredited area, room, group of rooms, or installation where SCI may be stored, used, discussed, and/or processed.

sensitive compartmented information (SCI): Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the DCI

pursuant to the special access provisions of Executive Order 12356 (e.g., COMINT, PHOTINT, etc.).

sensitive intelligence sources and methods: A collective term for those persons, organizations, things, conditions, or events that provide intelligence information and those means used in the collection, processing, and production of such information which, if compromised, would be vulnerable to counteraction that could reasonably be expected to reduce their ability to support US intelligence activities.

sensor: A technical device designed to detect and respond to one or more particular stimulae and that may record and/or transmit a resultant impulse for interpretation or measurement; often called a *technical sensor*. The term *special sensor* is used as a matter of convenience to refer to a highly classified or controlled technical sensor.

Service Cryptologic Elements (SCE): A term used to designate, separately or together, those elements of the US Army, Navy, and Air Force that perform cryptologic functions; also known as Service Cryptologic Agencies and Service Cryptologic Organizations.

side-looking airborne radar (SLAR): An airborne radar, viewing at right angles to the axis of the vehicle, which produces a presentation of terrain or targets.

SIGINT activity: Activity conducted for the purpose of producing signals intelligence. (Also see SIGINT-related activity.)

SIGINT-related activity: Any activity primarily intended for a purpose(s) other than signals intelligence, but which can be used to produce SIGINT, or which produces SIGINT as a by-product of its principal function(s). (Also see SIGINT activity.)

SIGINT technical information: Information concerning or derived from intercepted foreign transmissions or radiations that is composed of technical *information* (as opposed to *intelligence*) and that is required for the further collection or analysis of signals intelligence.

signal: (1) Any intentional transmission by visual and other electromagnetic, nuclear, or acoustical methods for either communications or noncommunications purposes. (2) In electronics, any transmitted electric impulse that is of interest in the particular context. (3) Anything intentionally transmitted by visual, acoustical, or electric means, consisting of one or more letters, words, characters, signal flags, visual displays, or special sounds with prearranged meanings.

signals intelligence (SIGINT): Intelligence information derived from signals intercept comprising, either individually or in combination, all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted.

Signals Intelligence (SIGINT) Committee: A body, supported by the Intelligence Community Staff, responsible for advising and assisting the DCI and the Director, NSA, on matters related to SIGINT and to monitor and promote the effective use of Intelligence Community SIGINT resources. (Refer to DCID 3/6.)

Signals Intelligence Requirements Validation and Evaluation Subcommittee (SIRVES): The subcommittee that acts for the SIGINT Committee in discharging the Committee's responsibilities for managing SIGINT requirements. The SIRVES is composed of representatives of all National Foreign Intelligence Board member agencies and Military Departments.

Signals Intelligence Security Regulation (SISR): A document that establishes basic policies, principles, and regulations governing the use, dissemination, and security of SIGINT.

signals security (SIGSEC): A term that includes communications security and electronics security and that encompasses measures intended to deny or counter hostile exploitation of electronic emissions.

signals security acquisition and analysis: The acquisition of electronic emissions and subsequent analysis to determine empirically the susceptibility of the emission to interception and exploitation by hostile intelligence services; it includes cataloging the transmission spectrum and taking signal parametric measurements as required, but does not include acquisition of information carried on the system; it is one of the techniques of signals security surveillance. (Also see signals security surveillance.)

signals security surveillance: The systematic examination of electronic emissions to determine the adequacy of signals security measures, to identify signals security deficiencies, to provide data from which to predict the effectiveness of proposed signals security measures, and to confirm the adequacy of such measures after implementation.

sleeper: An illegal or agent residing in a foreign country under orders to engage in no intelligence activities.

source: (1) A person, thing, or activity from which intelligence information is obtained. (2) In clandestine activities, a person (agent), normally a foreign national, in the employ of an intelligence activity for intelligence purposes. (3) In interrogation activities, any person who furnishes intelligence information, either with or without the knowledge that the information is being used for intelligence purposes. (Also see agent.)

Special Access Program (SAP): Any program established under Executive Order 12356 that imposes additional controls governing access to classified information involved with such programs beyond those required by normal management and safeguarding practices. These programs may include, but are not limited to, access approval, adjudication or investigative requirements, special designation of officials authorized to determine a need-to-know, or special lists of persons determined to have a need-to-know.

special activities: As defined in Executive Order No. 12333, activities conducted in support of national foreign policy objectives that are planned and executed so that the role of the US Government is not apparent or acknowledged publicly, but which are not intended to influence US political processes, public opinion, policies, or media and do not include diplomatic activities or the collection and production of intelligence or related support functions. (Also see covert action.)

Special Activities Office(r) (SAO): A control point for certain categories of compartmented information (the abbreviation is often used to refer to the compartmented information itself).

Special Coordination Committee (SCC): A committee established under the National Security Council that deals inter alia with the oversight of sensitive intelligence activities, such as covert actions, which are undertaken on Presidential authority.

Special Handling for Operational Procedures (SHOP): The provision of special imagery products for planning and executing military, paramilitary, and other operations by US forces.

special intelligence: An unclassified term used to designate a category of sensitive compartmented information. (Also see sensitive compartmented information.)

special intelligence communications (SPINTCOMM): A communications network for the handling of all special intelligence, consisting of facilities under the operational and technical control of the chief of intelligence in each of the Military Departments. The network is managed by the DIA under the technical and security specification criteria established and monitored by the NSA.

Special National Intelligence Estimate (SNIE): National Intelligence Estimates (NIEs) that are relevant to specific policy problems that need to be addressed in the immediate future. SNIEs are generally unscheduled, shorter, and prepared more quickly than NIEs and are coordinated within the Intelligence Community to the extent that time permits. (Also see National Intelligence Estimate.)

Special Security Office(r) (SSO): A control point for security procedures within any activity authorized access to sensitive compartmented information.

special sensor: Equipment on instrumental platforms and in installations designed to collect measurement and signature data that can be further processed into data usable by intelligence analysis. (Also see sensor.)

strategic intelligence: Intelligence that is required for the formulation of policy and military plans at national and international levels; it differs primarily from tactical intelligence in level of use, but may also vary in scope and detail.

strategic warning: Intelligence information or intelligence regarding the threat of the initiation of hostilities against the US or in which US forces may become involved; it may be received at any time prior to the initiation of hostilities.

subversion: Illegal action designed to undermine the military, economic, psychological, political strength, or morale of a regime.

subversive activity: Illegal activities that lend aid, comfort, and moral support to individuals, groups, or organizations that advocate the overthrow of incumbent governments by illegal means, usually by force and violence.

Support for the Analysts' File Environment (SAFE): A joint CIA/DIA online computer-based system, used separately by both CIA and DIA, designed to provide production analysts with pertinent and timely electronic mail, an electronic filing system, and a text retrieval capability for Intelligence Community reporting.

surveillance: The systematic observation or monitoring of places, persons, or things by visual, aural, electronic, photographic, or other means.

Tactical Cryptologic Program (TCP): An element of Tactical Intelligence and Related Activities (TIARA) which provides funding for SIGINT equipment supporting tactical requirements.

tactical intelligence: Foreign intelligence produced under the aegis of the Secretary of Defense and intended primarily to be responsive to the needs of military commanders in the field to maintain the readiness of operating forces for combat operations and to support the planning and conduct of combat operations. (Also see combat intelligence.)

Tactical Intelligence and Related Activities (TIARA): Intelligence and intelligence-related activities of the DoD that are not included in the NFIP.

tactical target materials (TTM): Those intelligence products which provide a graphic representation of a single or complex installation/target/facility having delineated boundaries, specific identification, and textual descriptions of geographic locations and physical characteristics. The current format for the TTM is the Automated Tactical Target Graphic.

tactical intelligence asset: An intelligence asset funded in DoD programs, the primary purpose of which is the collection or processing of intelligence information or the production of tactical intelligence. (Also see tactical intelligence and intelligence asset.)

tactical warning: A warning after initiation of a threatening or hostile act based on an evaluation of information from all available sources. Also called integrated tactical warning.

target: (1) A country, area, installation, organization, weapon system, military force, situation (political or economic), signal, person, or other entity against which intelligence operations are conducted. (2) (Military usage.) A geographical area, system, complex, or installation planned for capture, destruction, or disruption by military force.

target intelligence: Intelligence that portrays and locates the components of a target or target complex and indicates its identification, vulnerability, and relative importance.

tasking: The assignment or direction of an individual or activity to perform in a specified way to achieve an objective or goal.

technical ELINT (TECHELINT): A form of ELINT that provides detailed knowledge of the technical characteristics of a given emitter, which permits estimation of its primary function, capabilities, and modes of operation (including malfunctions) as well as its specific role within a complex weapons system or defense network.

technical intelligence (TI): Intelligence on the characteristics and performance of foreign weapons and equipment; a part of scientific and technical intelligence and distinct from order of battle.

technical penetration: A deliberate penetration of a secure area by technical means to gain unauthorized interception of information-bearing energy.

technical sensor: See sensor.

technical SIGINT: Intelligence information that provides detailed knowledge of the technical characteristics of a given emitter and thus permits estimates to be made about its primary function, capabilities, modes of operation (including malfunctions), and state of the art, as well as its specific role within a complex weapon system or defense network; it is a contributor to technical intelligence.

technical surveillance countermeasures (TSCM): Techniques and measures to detect and neutralize a wide variety of hostile penetration technologies that are used to obtain unauthorized access to classified and sensitive information. Technical penetrations include the employment of optical, electro-optical, electromagnetic, fluidic, and acoustic means, as the sensor and transmission medium, or the use of various types of stimulation or modification to equipment or building components for the direct or indirect transmission of information meant to be protected.

technical surveillance countermeasures (TSCM) monitor: A limited TSCM inspection, normally provided in conjunction with sensitive briefings, conferences, and seminars, that consists basically of an examination of portions of the electromagnetic spectrum and a thorough physical and visual examination of the area.

technical surveillance device: A device covertly installed to monitor (visually, audibly, or electronically) sensitive activities and/or information processing within a target area.

technical surveillance hazard: A condition that could permit the technical penetration of an area wherein sensitive information might be compromised. A hazard may be caused by equipment, which by reasons of its normal design and installation, or by reasons of faulty fabrication, installation, operations or maintenance, or by reasons of accidental damage, could facilitate the unintentional transmission of sensitive information.

technology transfer: All movements of advanced US and equivalent Western technology and equipment that enhance the military and economic capabilities of recipient countries that have implications for US national security.

technology transfer intelligence: The collection, processing, analysis, production, and dissemination activities of the Intelligence Community designed to support US Government departments and agencies with policy and enforcement responsibilities related to the area of technology transfer.

Technology Transfer Intelligence Committee (TTIC): A DCI advisory committee that serves as the focal point within the Intelligence Community on all technology transfer issues. (Refer to DCID 3/13.)

telecommunications: Any transmission, emission, or reception of signs, signals, writing, images, and sounds or information of any nature by wire, radio, visual, or other electromagnetic systems.

telemetry intelligence (TELINT): Technical and intelligence information derived from intercept, processing, and analysis of foreign telemetry; a subcategory of foreign instrumentation signals intelligence.

teleprocessing: The overall function of an information transmission system that combines telecommunications, automatic data processing, and man-machine interface equipment and their interaction as an integrated whole.

TEMPEST: An unclassified term referring to technical investigations for compromising emanations from electrically operated, information processing equipment; they are conducted in support of emanations and emission security.

terrain intelligence: Processed information on the military significance of natural and manmade characteristics of an area.

terrorist organization: A group that engages in terrorist activities. (Also see international terrorist activity.)

Theater Intelligence Architecture Program (TIAP): A program encompassing each Unified and Specified Command's mid- and long-range plan for providing intelligence required to carry out warfighting missions. Each Command's intelligence architecture plan is based on operational requirements and describes current and future intelligence flows, organizations, resources, and capabilities to meet assigned intelligence objectives. The plans also assess shortfalls and provide a strategy for overcoming deficiencies.

threat: The extant military, economic, and political capabilities of a foreign nation or entity coupled with the aggressive intentions to use such capabilities to undertake any action whose consequence would be detrimental to the interests of the United States.

Time-Sensitive Requirement or Report (TSR): A request made by a consumer to NSA or other collection agency for immediate information that is generated in response to an unexpected or unusual high-interest event or crisis situation that is time critical. The TSR is the requirements vehicle used when a response by the US SIGINT System is required within 48 hours or less.

TOP SECRET (TS): Security classification applied to information which, if disclosed in an unauthorized manner, could reasonably be expected to cause exceptionally grave damage to national security.

traffic analysis (TA): The cryptologic discipline that develops information from communications about the composition and operation of communications structures and the organizations they serve. The process involves the study of traffic and related materials, and the reconstruction of communication plans to produce SIGINT.

transmission security (TRANSEC): The component of communications security that results from all measures designed to protect transmissions from interception and from exploitation by means other than cryptanalysis.

triple agent: An agent who serves three services in an agent capacity but who, like a double agent, wittingly or unwittingly withholds significant information from two services at the instigation of the third service.

unauthorized disclosure: See compromise.

unilevel security: (For automated information systems.) (1) Provisions for the safeguarding of all material within a single information handling system in accordance with the highest level of classification and most restrictive dissemination caveats assigned to any material contained therein. (2) A security yardstick that is attained when all users of an information system have a national intelligence clearance and have signed nondisclosure agreements for all information in the system—also called *system high mode of operation.* (Also see **multilevel security.**)

United States SIGINT System (USSS): An entity that is comprised of the NSA (including assigned military personnel), elements of the Military Departments and the CIA performing SIGINT activities, and elements of any other department or agency that may from time to time be authorized by the National Security Council to perform SIGINT activities during the time when such elements are so authorized; it is governed by the United States Signals Intelligence Directives System.

upgrade: To determine that certain classified information requires, in the interest of national security, a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such higher degree. (Also see **classification.**)

validation: (1) A process normally associated with the collection of intelligence information that provides official status to an identified requirement and confirms that the requirement is appropriate for a given collector and has not previously been satisfied. (Also see **collection requirement.**) (2) In hypothesis testing, a means of establishing the accuracy of the measuring instrument, or the validity of the test, in measuring the relevant variables.

verification: The process used by policymaking officials to judge whether or not activities of another party are in compliance with arms control agreements. While verification judgments begin with monitoring assessments, policymaking officials also consider political and military risks and the application of safeguards.

walk-in: A person who, on his own initiative, makes contact with a representative of a foreign country and who volunteers intelligence information and/or requests political asylum. (Also see **disaffected person.**)

warning: A communication and acknowledgment of dangers implicit in a wide spectrum of activities by potential opponents ranging from routine defense measures, to substantial increases in readiness and force preparedness, to acts of terrorism or political, economic, or military provocation. (Also see **strategic warning.**)

WARNING NOTICE-INTELLIGENCE SOURCES OR METHODS INVOLVED (WNINTEL): Security designation used to identify classified intelligence whose sensitivity requires constraints on its further dissemination and use. This designation is used on intelligence that identifies or would reasonably permit identification of an intelligence source or method that is susceptible to countermeasures that could nullify or reduce its effectiveness. May be abbreviated "WNINTEL" or "WN."

Wartime Reserve Modes (WARM): Characteristics and operating procedures of sensors, communications, navigation aids, weapons, and countermeasures that will contribute to military effectiveness or deception if unknown to or misunderstood by opposing forces before combat.

Weapon and Space Systems Intelligence Committee (WSSIC): An advisory committee responsible for advising and assisting the DCI in the production of national intelligence on foreign weapon and space systems. (Refer to DCID 3/11.)

zone of control: Spherical zone around a piece of equipment where access by unauthorized personnel is not permitted without escort.

SECTION II

ACRONYMS AND ABBREVIATIONS

ACINT	Acoustical Intelligence
ACSI	Assistant Chief of Staff/Intelligence (Air Force)
AFIA	Air Force Intelligence Agency
AFMIC	Armed Forces Medical Intelligence Center
AI	Artificial Intelligence
AIA	Army Intelligence Agency
AIRES	Advanced Imagery Requirements and Exploitation System
ALE	AIRES Life Extension
ATTG	Automated Tactical Target Graphic
CAMS	COMIREX Automated Management System
CAP	Countermeasures Advisory Panel
C³I	Command, Control, Communications, and Intelligence
CCD	Camouflage, Concealment, and Deception
CCF	Collection Coordination Facility
CCISCMO	Community Counterintelligence and Security Countermeasures Office
CCP	Consolidated Cryptologic Program
CI	Counterintelligence
CIA	Central Intelligence Agency
CIAP	Central Intelligence Agency Program
CIFAX	Enciphered Facsimile
CIP	Critical Intelligence Parameters
CIPHONY	Enciphered Telephone
CIPR	Consolidated Intelligence Production Requirement
CIR	Continuing Intelligence Requirements
CIRIS	Consolidated Intelligence Resources Information System
COCOM	Coordinating Committee for Multilateral Strategic Export
COFIR	Compendium of Future Intelligence Requirements
COINS	Community On-Line Intelligence System
COMINT	Communications Intelligence
COMIREX	Committee on Imagery Requirements and Exploitation
COMPUSEC	Computer Security
COMSEC	Communications Security
CONTEXT	Conferencing and Text Manipulation System
COVCOM	Covert Communications
CRITIC	Critical Intelligence Message
CRITICOMM	Critical Intelligence Communications System
DAO	Defense Attache Office
DARPA	Defense Advanced Research Projects Agency
DCA	Defense Communications Agency
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive

DCSINT	Deputy Chief of Staff for Intelligence (Army)
D&D	Denial and Deception
DDAC	Foreign Denial and Deception Analysis Committee
DDCI	Deputy Director of Central Intelligence
DEA	Drug Enforcement Administration
DEFSMAC	Defense Special Missile and Astronautic Center
DESIST	Decision Support & Information System on Terrorism
DF	Direction Finding
DIA	Defense Intelligence Agency
DIAC	Defense Intelligence Analysis Center
DIAOLS	DIA On-Line System
DIC	Defense Intelligence College
DIE	Defense Intelligence Estimate
DIO	Defense Intelligence Officer
DIRNSA	Director, National Security Agency
DIS	Defense Investigative Service
DIVISION	Enciphered Television
DN	Duplicate Negative
DNI	Director of Naval Intelligence
DoD	Department of Defense
DoDIIS	DoD Intelligence Information System
DP	Duplicate Positive
ECCM	Electronic Counter-Countermesaures
ECM	Electronic Countermeasures
EEI	Essential Elements of Information
E&E	Evasion and Escape
EIC	Economic Intelligence Committee
ELECTRO-OPTINT	Electro-optical Intelligence
ELINT	Electronic Intelligence
ELSEC	Electronic Security
EMCON	Emission Control
EMSEC	Emanations Security
EOB	Electronic Order of Battle
ESC	Electronic Security Command (Air Force)
ESM	Electronic Warfare Support Measures
EW	Electronic Warfare
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FCI	Foreign Counterintelligence
FDDAC	Foreign Denial and Deception Analysis Committee
FEMA	Federal Emergency Management Agency
FI	Foreign Intelligence
FIPC	Foreign Intelligence Priorities Committee
FIRCAP	Foreign Intelligence Requirements Categories and Priorities
FIS	Foreign Instrumentation Signals
FISINT	Foreign Instrumentation Signals Intelligence
FLC	Foreign Language Committee
FLIR	Forward-Looking Infrared
FMA	Foreign Materiel Acquisition
FME	Foreign Materiel Exploitation
FMP	Foreign Materiel Program

FSTC	Foreign Science and Technology Center (Army)
FTD	Foreign Technology Division (Air Force)
FORMAT or FM	Foreign Materiel
FOSIC	Fleet Ocean Surveillance Information Center
GDIP	General Defense Intelligence Program
GMI	General Medical Intelligence
HFDF	High Frequency Direction Finding
HOIS	Hostile Intelligence Service
HPSCI	House Permanent Select Committee on Intelligence
HUMINT	Human Intelligence
IA	Imagery Analyst
IC	Intelligence Community
ICR	Intelligence Collection Requirement
ICRS	Imagery Collection Requirements Subcommittee (COMIREX)
ICS	Intelligence Community Staff
IDC	Interagency Defector Committee
IDS	Intrusion Detection Systems
IHC	Information Handling Committee
II	Imagery Interpretation
IIM	Interagency Intelligence Memorandum
IIR	Intelligence Information Report
ILC	International Lines of Communications
IMINT	Imagery Intelligence
INDICOM	Indications and Warning Communications
INFOSEC	Information Security
INR	Bureau of Intelligence and Research, Department of State
INSCOM	US Army Intelligence and Security Command
INTELSAT	International Telecommunications Satellite
IOB	Intelligence Oversight Board
IPC	Intelligence Producers Council
IPCS	Intelligence Producers Council Staff
IR	Infrared
IRA	Intelligence-Related Activities
IRDC	Intelligence Research & Development Council
ISP	Intelligence Support Plan
ITAC	Intelligence Threat and Analysis Center (Army)
ITC	Interagency Training Center
ITL	Interagency Telephone Laboratory
I&W	Indications and Warning
JAEIC	Joint Atomic Energy Intelligence Committee
JCS	Joint Chiefs of Staff
JEWC	Joint Electronic Warfare Center
JINTACCS	Joint Interoperability Tactical Command and Control System
LASINT	Laser Intelligence
LIC	Low-Intensity Conflict
LITINT	Literature Intelligence
LPI	Low Probability of Intercept

MASINT	Measurement and Signature Intelligence
MBFR	Mutual and Balanced Force Reduction
MEDINT	Medical Intelligence
MI	Military Intelligence
MIB	Military Intelligence Board
MSIC	Missile and Space Intelligence Center (Army)
NAVINTCOM	Naval Intelligence Command
NAVOPINTCEN	Navy Operational Intelligence Center
NAVTECHINTCEN	Naval Technical Intelligence Center
NCIS	National Counterintelligence Strategy
NDA	Nondisclosure Agreement
NEL	National Exploitation Laboratory
NFIB	National Foreign Intelligence Board
NFIC	National Foreign Intelligence Council
NFIP	National Foreign Intelligence Program
NHCP	National HUMINT Collection Plan
NIC	National Intelligence Council, Naval Intelligence Command
NID	National Intelligence Daily
NIE	National Intelligence Estimate
NIIRS	National Imagery Interpretability Rating Scale
NIO	National Intelligence Officer
NITs	National Intelligence Topics
NMIC	National Military Intelligence Center
NOCONTRACT	NOT RELEASABLE TO CONTRACTORS/CONSULTANTS
NOFORN or NF	NOT RELEASABLE TO FOREIGN NATIONALS
NOIWON	National Operations and Intelligence Watch Officer Network
NPHR	National Foreign Intelligence Plan for Human Resources
NPIC	National Photographic Interpretation Center
NRIS	National Radar Interpretability Scale
NSA	National Security Agency
NSC	National Security Council
NSCID	National Security Council Intelligence Directive
NSD	National Security Directive
NSG	Naval Security Group
NSIC	Navy Security and Investigation Command
NSOC	National SIGINT Operations Center
NSRL	National SIGINT Requirements List
NSRS	National SIGINT Requirements System
NTISSC	National Telecommunications and Information Systems Security Committee
NTPC	National Telemetry Processing Center
NUCINT	Nuclear Intelligence
OADR	Originating Agency Determination Required
OB	Order of Battle
ON	Original Negative
OPCON	Operational Control
OPELINT	Operational Electronic Intelligence
OPINTEL	Operational Intelligence
OPSEC	Operations Security

OPTINT	Optical Intelligence
ORCON	DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR
OSIA	On-Site Inspection Agency
OSIS	Ocean Surveillance Information System
PFIAB	President's Foreign Intelligence Advisory Board
PHOTINT	Photographic Intelligence
PI	Photographic Interpretation or Photographic Interpreter
PIR	Primary Imaging Record
PNG	Persona Non Grata
PRCSO	Peacetime Reconnaissance and Certain Sensitive Operations
PROPIN	CAUTION-PROPRIETARY INFORMATION INVOLVED
PSYOP	Psychological Operations
RADINT	Radar Intelligence
RECCE or RECON	Reconnaissance
RFI	Request for Information
RINT	Radiation Intelligence
RMS	Requirements Management System
S&T	Science and Technology
SA	Signals Analysis
SAFE	Support for the Analysts File Environment
SAO	Special Activities Office
SAP	Special Access Program
SAR	Synthetic Aperture Radar
SCA	Service Cryptologic Agencies
SCC	Special Coordination Committee
SCE	Service Cryptologic Element
SCI	Sensitive Compartmented Information or Source Code Indicator
SCIF	SCI Facility
SCM	Security Countermeasures
SCO	Service Cryptologic Organizations
SDC	Strategic Defense Command (Army)
SHOP	Special Handling for Operational Purposes
SI	Special Intelligence
SIG	Senior Interagency Group
SIGINT	Signals Intelligence
SIGSEC	Signals Security
SIO	Senior Intelligence Officer
SIRVES	SIGINT Requirements Validation and Evaluation Subcommittee (of SIGINT Committee)
SISR	SIGINT Security Regulation
SLAR	Side-Looking Airborne Radar
SNIE	Special National Intelligence Estimate
SOIC	Senior Official of the Intelligence Community
SOSUS	Sound Surveillance System
SOTA	SIGINT Operational Tasking Authority
SPINTCOMM	Special Intelligence Communications

SSCI	Senate Select Committee on Intelligence
SSO	Special Security Officer
STAP	Science and Technology Advisory Panel
STAR	System Threat Assessment Report
STIC	Scientific and Technical Intelligence Committee
TA	Traffic Analysis
TACINTEL	Tactical Intelligence
TCP	Tactical Cryptological Program
TECHELINT	Technical ELINT
TELINT	Telemetry Intelligence
TI	Technical Intelligence
TIAP	Theater Intelligence Architecture Program
TIARA	Tactical Intelligence and Related Activities
TRANSEC	Transmission Security
TS	Top Secret
TSCM	Technical Surveillance Countermeasures
TSR	Time-Sensitive Requirement
TTIC	Technology Transfer Intelligence Committee
USIC	United States Intelligence Community
USILO	US Imagery Liaison Officer
USSID	United States Signals Intelligence Directive
USSS	United States SIGINT System
VIDINT	Video Intelligence
VISINT	Visual Intelligence
WARM	Wartime Reserve Modes
WHCA	White House Communications Agency
WNINTEL	Warning Notice-Intelligence Sources and Methods Involved
WSSIC	Weapon and Space Systems Intelligence Committee
WWIMS	Worldwide Warning Indicator Monitoring System
WWMCCS	Worldwide Military Command and Control Systems

SECTION III

INDEX OF OTHER INTELLIGENCE GLOSSARIES AND PUBLICATIONS

Catalog of Abbreviations and Brevity Codes, Army Regulation 310-25.

Combat Electronic Warfare and Intelligence, Army Field Manual 34-1.

Combat Intelligence, Army Field Manual 30-5.

COMIREX Imagery Policy Series, 1988 (and revisions)

Communications Security, Army Regulation 530-2.

Defense Intelligence Lexicon, DVP-2600-1828-88, 1988.

Defense Intelligence Collection Requirements Manual, DIA, August 1981.

DoD Manual for Standard Data Elements, DoD 5000.12-M, October 1983.

Dictionary of Military and Associated Terms, JCS Pub 1-02, June 1987.

Dictionary of Naval Abbreviations, Naval Institute Press, 1984.

Dictionary of United States Army Terms, Army Regulation 310-25.

Directory: Information Resources Based on Foreign Media and Publications, DCI HUMINT Committee, July 1985.

Doctrine for Intelligence Support to Joint Operations (Draft), JCS Pub 2-0, 1989.

Engineer Intelligence, Army Field Manual 5-30.

Final Report of the Select Committee to Study Governmental Operations With Respect to Intelligence Activities, United States Senate, Together with Additional Supplemental and Separate Views, April 1976.

Glossary of SIGINT Collection Terminology, National Security Agency, August 1986.

House Resolution 658, (Establishes House Permanent Select Committee on Intelligence), November 1977.

Index to Publications, Department of Army Pamphlet DAPAM 25-30, 1988.

Intelligence Data Elements Authorized Standards (IDEAS), DRS-2600-1696-83, October 1983.

Intelligence Dissemination and Production Support, Army Regulation 381-19, 16 February 1988.

Intelligence Interrogation, Army Field Manual 30-15.

Joint Intelligence Estimate for Planning (JIEP), SM-580-88, JCS, 25 July 1988.

Limitations and Procedures in Signals Intelligence Operations of the USSS, USSID 18, October 1980.

Military Intelligence, Army Regulation 381 Series.

Military Symbols, Army Field Manual 21-30.

Modern Data Communications Concepts, Language and Media, William P. Davenport, Hayden Book Co., Inc., 1971.

National Communications Security Glossary, NSA, September 1982.

National Foreign Intelligence Plan for Human Resources, NFIB D/27.7/5, 1977.

National Security Information, Executive Order No. 12356, April 1982.

Handbook for the National SIGINT Requirements System, July 1988.

NATO Glossary of Terms and Definitions (English and French), AAP-6(Q), March 1986.

Operations, Army Field Manual 100-5.

Operations and Signal Security, Army Regulation 530 Series.

Psychological Operations: US Army Doctrine, Army Field Manual 33-1.

Physical Security, Army Field Manual 19-30.

Security, Army Regulation 380 Series.

Security, The Use and Dissemination of Communications Intelligence, USAFINTEL 201-1, March 1985.

Senate Resolution 400, (Establishes the Senate Select Committee on Intelligence), June 1977.

Sensitive Compartmented Information Security Manual: Administrative Security, DoD C-5105.21-M-1, January 1985.

Sensitive Compartmented Information Security Manual: Communications Intelligence Policy, DoD TS-5105.21-M-2, July 1985.

Sensitive Compartmented Information Security Manual: TK Policy, DoD TS-5105.21-M-3, November 1985.

SIGINT Security, NSA, USSID 3, May 1986.

Signals Intelligence, Army Regulation 381-3.

SIGSEC Techniques, Army Field Manual 32-6.

Statement of Intelligence Interest, DoD Document No. 05990.

Technical Intelligence, Army Field Manual 30-16.

Threat Support to US Army Force, Combat, and Material Development, Army Regulation 381-11.

US Army Counterintelligence Activities, Army Regulation 381-20.

US Army Intelligence Activities, Army Regulation 381-10.

United States Intelligence Activities, Executive Order No. 12333, December 1981.

US Army Requirements for Weather Service Support, Army Regulation 115-12.