2011 Administrative Law Supplement for

U.S. Intelligence Law

DAVID ALAN JORDAN

IntelligenceLaw.com®

2011 Administrative Law Supplement for

U.S. Intelligence Law

(November 2011)

By

David Alan Jordan
Editor-in-Chief/Principal Lecturer
IntelligenceLaw.com

IntelligenceLaw.com Creative Commons Supplement Series

IntelligenceLaw.com®

United States of America, 2011

To the Center for
Democracy &
Technology and
OpenCRS.com
[www.cdt.org &
http://opencrs.com]

Preface

This supplement contains the administrative rules most relevant to the courses on IntelligenceLaw.com. Specifically, this supplement contains a selection of presidential orders, agency directives, administrative guidelines, and court rules that govern domestic intelligence operations affecting United States persons. This publication is a work in progress. A more comprehensive second edition is scheduled for release in 2012.

DAVID ALAN JORDAN

November, 2011

Summary of Contents

Table of Contents

Administrative Law Supplement for

U.S. Intelligence Law

(November 2011)

IntelligenceLaw.com Creative Commons Supplement Series

I. PRESIDENTIAL RULES

Executive Orders Relevant to U.S. Intelligence Law

Executive Order 12,333: United States Intelligence Activities

As Amended Through January 1, 2010

Exec. Order No. 12,333, United States Intelligence Activities, 46 Fed. Reg. 59941, 3 C.F.R. 200 *et seq*. (Dec. 4, 1981), *as amended by* Exec. Order. No. 13,284, 68 Fed. Reg. 4077 (Jan. 23, 2003); Exec. Order No. 13,355, 69 Fed. Reg. 53593 (Aug. 27, 2004); and Exec. Order No. 13,470, 73 Fed. Reg. 45325 (July 30, 2008), *available at* http://www.intelligencelaw.com/library/admin/html/eo_12333_2010.html.

Table of Contents

Preamble

Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence available. For that purpose, by virtue of the authority vested in me by the Constitution and the laws of the United States of America, including the National Security Act of 1947 [50 U.S.C. §§ 401 et seq.], as amended (Act), and as President of the United States of America, in order to provide for the effective conduct of United States intelligence activities and the protection of constitutional rights, it is hereby ordered as follows:

PART 1: Goals, Directions, Duties, and Responsibilities with Respect to United States Intelligence Efforts

1.1 Goals

The United States intelligence effort shall provide the President, the National Security Council, and the Homeland Security Council with the necessary information on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.

- (a) All means, consistent with applicable Federal law and this order, and with full consideration of the rights of United States persons, shall be used to obtain reliable intelligence information to protect the United States and its interests.
- (b) The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.
- (c) Intelligence collection under this order should be guided by the need for information to respond to intelligence priorities set by the President.
- (d) Special emphasis should be given to detecting and countering:

    - (1) Espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;
    - (2) Threats to the United States and its interests from terrorism; and
    - (3) Threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction.
- (e) Special emphasis shall be given to the production of timely, accurate, and insightful reports, responsive to decisionmakers in the executive branch, that draw on all appropriate sources of information, including open source information, meet rigorous analytic standards, consider diverse analytic viewpoints, and accurately represent appropriate alternative views.
- (f) State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take into account the responsibilities and requirements of State, local, and tribal governments and, as appropriate, private sector entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.
- (g) All departments and agencies have a responsibility to prepare and to provide intelligence in a manner that allows the full and free exchange of information, consistent with applicable law and presidential guidance.

1.2 The National Security Council

(a) Purpose

The National Security Council (NSC) shall act as the highest ranking executive branch entity that provides support to the President for review of, guidance for, and direction to the conduct of all foreign intelligence, counterintelligence, and covert action, and attendant policies and programs.

(b) Covert Action and Other Sensitive Intelligence Operations

The NSC shall consider and submit to the President a policy recommendation, including all dissents, on each proposed covert action and conduct a periodic review of ongoing covert action activities, including an evaluation of the effectiveness and consistency with current national policy of such activities and consistency with applicable legal requirements. The NSC shall perform such other functions related to covert action as the President may direct, but shall not undertake the conduct of covert actions. The NSC shall also review proposals for other sensitive intelligence operations.

1.3 Director of National Intelligence

Subject to the authority, direction, and control of the President, the Director of National Intelligence (Director) shall serve as the head of the Intelligence

Community, act as the principal adviser to the President, to the NSC, and to the Homeland Security Council for intelligence matters related to national security, and shall oversee and direct the implementation of the National Intelligence Program and execution of the National Intelligence Program budget. The Director will lead a unified, coordinated, and effective intelligence effort. In addition, the Director shall, in carrying out the duties and responsibilities under this section, take into account the views of the heads of departments containing an element of the Intelligence Community and of the Director of the Central Intelligence Agency.

- (a) Except as otherwise directed by the President or prohibited by law, the Director shall have access to all information and intelligence described in section 1.5(a) of this order. For the purpose of access to and sharing of information and intelligence, the Director:
    - (1) Is hereby assigned the function under section 3(5) of the Act, to determine that intelligence, regardless of the source from which derived and including information gathered within or outside the United States, pertains to more than one United States Government agency; and
    - (2) Shall develop guidelines for how information or intelligence is provided to or accessed by the Intelligence Community in accordance with section 1.5(a) of this order, and for how the information or intelligence may be used and shared by the Intelligence Community. All guidelines developed in accordance with this section shall be approved by the Attorney General and, where applicable, shall be consistent with guidelines issued pursuant to section 1016 of the Intelligence Reform and Terrorism Protection Act of 2004 [6 U.S.C. § 485] (Public Law 108-458) (IRTPA).
- (b) In addition to fulfilling the obligations and responsibilities prescribed by the Act, the Director:
    - (1) Shall establish objectives, priorities, and guidance for the Intelligence Community to ensure timely and effective collection, processing, analysis, and dissemination of intelligence, of whatever nature and from whatever source derived;
    - (2) May designate, in consultation with affected heads of departments or Intelligence Community elements, one or more Intelligence Community elements to develop and to maintain services of common concern on behalf of the Intelligence Community if the Director determines such services can be more efficiently or effectively accomplished in a consolidated manner;
    - (3) Shall oversee and provide advice to the President and the NSC with respect to all ongoing and proposed covert action programs;
    - (4) In regard to the establishment and conduct of intelligence arrangements and agreements with foreign governments and international organizations:

        - (A) May enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations;
        - (B) Shall formulate policies concerning intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations; and
        - (C) Shall align and synchronize intelligence and counterintelligence foreign relationships among the elements of the Intelligence Community to further United States national security, policy, and intelligence objectives;
    - (5) Shall participate in the development of procedures approved by the Attorney General governing criminal drug intelligence activities abroad to ensure that these activities are consistent with foreign intelligence programs;
    - (6) Shall establish common security and access standards for managing and handling intelligence systems, information, and products, with special emphasis on facilitating:
        - (A) The fullest and most prompt access to and dissemination of information and intelligence practicable, assigning the highest priority to detecting, preventing, preempting, and disrupting terrorist threats and activities against the United States, its interests, and allies; and
        - (B) The establishment of standards for an interoperable information sharing enterprise that facilitates the sharing of intelligence information among elements of the Intelligence Community;
    - (7) Shall ensure that appropriate departments and agencies have access to intelligence and receive the support needed to perform independent analysis;
    - (8) Shall protect, and ensure that programs are developed to protect, intelligence sources, methods, and activities from unauthorized disclosure;
    - (9) Shall, after consultation with the heads of affected departments and agencies, establish guidelines for Intelligence Community elements for:
        - (A) Classification and declassification of all intelligence and intelligence-related information classified under the authority of the Director or the authority of the head of a department or Intelligence Community element; and
        - (B) Access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered, to include intelligence originally classified by the head of a department or Intelligence Community element, except that access to and dissemination of information concerning United States

persons shall be governed by procedures developed in accordance with Part 2 of this order;

- (10) May, only with respect to Intelligence Community elements, and after consultation with the head of the originating Intelligence Community element or the head of the originating department, declassify, or direct the declassification of, information or intelligence relating to intelligence sources, methods, and activities. The Director may only delegate this authority to the Principal Deputy Director of National Intelligence;
- (11) May establish, operate, and direct one or more national intelligence centers to address intelligence priorities;
- (12) May establish Functional Managers and Mission Managers, and designate officers or employees of the United States to serve in these positions.
    - (A) Functional Managers shall report to the Director concerning the execution of their duties as Functional Managers, and may be charged with developing and implementing strategic guidance, policies, and procedures for activities related to a specific intelligence discipline or set of intelligence activities; set training and tradecraft standards; and ensure coordination within and across intelligence disciplines and Intelligence Community elements and with related non-intelligence activities. Functional Managers may also advise the Director on: the management of resources; policies and procedures; collection capabilities and gaps; processing and dissemination of intelligence; technical architectures; and other issues or activities determined by the Director.
        - (i) The Director of the National Security Agency is designated the Functional Manager for signals intelligence;
        - (ii) The Director of the Central Intelligence Agency is designated the Functional Manager for human intelligence; and
        - (iii) The Director of the National Geospatial-Intelligence Agency is designated the Functional Manager for geospatial intelligence.
    - (B) Mission Managers shall serve as principal substantive advisors on all or specified aspects of intelligence related to designated countries, regions, topics, or functional issues;
- (13) Shall establish uniform criteria for the determination of relative priorities for the transmission of critical foreign intelligence, and advise the Secretary of Defense concerning the communications requirements of the Intelligence Community for the transmission of such communications;

- (14) Shall have ultimate responsibility for production and dissemination of intelligence produced by the Intelligence Community and authority to levy analytic tasks on intelligence production organizations within the Intelligence Community, in consultation with the heads of the Intelligence Community elements concerned;
- (15) May establish advisory groups for the purpose of obtaining advice from within the Intelligence Community to carry out the Director's responsibilities, to include Intelligence Community executive management committees composed of senior Intelligence Community leaders. Advisory groups shall consist of representatives from elements of the Intelligence Community, as designated by the Director, or other executive branch departments, agencies, and offices, as appropriate;
- (16) Shall ensure the timely exploitation and dissemination of data gathered by national intelligence collection means, and ensure that the resulting intelligence is disseminated immediately to appropriate government elements, including military commands;
- (17) Shall determine requirements and priorities for, and manage and direct the tasking, collection, analysis, production, and dissemination of, national intelligence by elements of the Intelligence Community, including approving requirements for collection and analysis and resolving conflicts in collection requirements and in the tasking of national collection assets of Intelligence Community elements (except when otherwise directed by the President or when the Secretary of Defense exercises collection tasking authority under plans and arrangements approved by the Secretary of Defense and the Director);
- (18) May provide advisory tasking concerning collection and analysis of information or intelligence relevant to national intelligence or national security to departments, agencies, and establishments of the United States Government that are not elements of the Intelligence Community; and shall establish procedures, in consultation with affected heads of departments or agencies and subject to approval by the Attorney General, to implement this authority and to monitor or evaluate the responsiveness of United States Government departments, agencies, and other establishments;
- (19) Shall fulfill the responsibilities in section 1.3(b)(17) and (18) of this order, consistent with applicable law and with full consideration of the rights of United States persons, whether information is to be collected inside or outside the United States;
- (20) Shall ensure, through appropriate policies and procedures, the deconfliction, coordination, and integration of all intelligence activities conducted by an Intelligence Community element or

funded by the National Intelligence Program. In accordance with these policies and procedures:

- (A) The Director of the Federal Bureau of Investigation shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities inside the United States;
- (B) The Director of the Central Intelligence Agency shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities outside the United States;

- (C) All policies and procedures for the coordination of counterintelligence activities and the clandestine collection of foreign intelligence inside the United States shall be subject to the approval of the Attorney General; and
- (D) All policies and procedures developed under this section shall be coordinated with the heads of affected departments and Intelligence Community elements;

- (21) Shall, with the concurrence of the heads of affected departments and agencies, establish joint procedures to deconflict, coordinate, and synchronize intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program, with intelligence activities, activities that involve foreign intelligence and security services, or activities that involve the use of clandestine methods, conducted by other United States Government departments, agencies, and establishments;
- (22) Shall, in coordination with the heads of departments containing elements of the Intelligence Community, develop procedures to govern major system acquisitions funded in whole or in majority part by the National Intelligence Program;
- (23) Shall seek advice from the Secretary of State to ensure that the foreign policy implications of proposed intelligence activities are considered, and shall ensure, through appropriate policies and procedures, that intelligence activities are conducted in a manner consistent with the responsibilities pursuant to law and presidential direction of Chiefs of United States Missions; and
- (24) Shall facilitate the use of Intelligence Community products by the Congress in a secure manner.

- (c) The Director's exercise of authorities in the Act and this order shall not abrogate the statutory or other responsibilities of the heads of departments of the United States Government or the Director of the Central Intelligence Agency. Directives issued and actions taken by the Director in the exercise of the Director's authorities and responsibilities to integrate, coordinate, and make the Intelligence Community more

effective in providing intelligence related to national security shall be implemented by the elements of the Intelligence Community, provided that any department head whose department contains an element of the Intelligence Community and who believes that a directive or action of the Director violates the requirements of section 1018 of the IRTPA [50 U.S.C. § 403 note] or this subsection shall bring the issue to the attention of the Director, the NSC, or the President for resolution in a manner that respects and does not abrogate the statutory responsibilities of the heads of the departments.

- (d) Appointments to certain positions.
    - (1) The relevant department or bureau head shall provide recommendations and obtain the concurrence of the Director for the selection of: the Director of the National Security Agency, the Director of the National Reconnaissance Office, the Director of the National Geospatial-Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for Intelligence and Research, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury, and the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation. If the Director does not concur in the recommendation, the department head may not fill the vacancy or make the recommendation to the President, as the case may be. If the department head and the Director do not reach an agreement on the selection or recommendation, the Director and the department head concerned may advise the President directly of the Director's intention to withhold concurrence.
    - (2) The relevant department head shall consult with the Director before appointing an individual to fill a vacancy or recommending to the President an individual be nominated to fill a vacancy in any of the following positions: the Under Secretary of Defense for Intelligence; the Director of the Defense Intelligence Agency; uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps above the rank of Major General or Rear Admiral; the Assistant Commandant of the Coast Guard for Intelligence; and the Assistant Attorney General for National Security.
- (e) Removal from certain positions.
    - (1) Except for the Director of the Central Intelligence Agency, whose removal the Director may recommend to the President, the Director and the relevant department head shall consult on the removal, or recommendation to the President for removal, as the case may be, of: the Director of the National Security Agency, the Director of the National Geospatial-Intelligence Agency, the Director of the Defense Intelligence Agency, the Under Secretary of Homeland

Security for Intelligence and Analysis, the Assistant Secretary of State for Intelligence and Research, and the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury. If the Director and the department head do not agree on removal, or recommendation for removal, either may make a recommendation to the President for the removal of the individual.

- (2) The Director and the relevant department or bureau head shall consult on the removal of: the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Director of the National Reconnaissance Office, the Assistant Commandant of the Coast Guard for Intelligence, and the Under Secretary of Defense for Intelligence. With respect to an individual appointed by a department head, the department head may remove the individual upon the request of the Director; if the department head chooses not to remove the individual, either the Director or the department head may advise the President of the department head's intention to retain the individual. In the case of the Under Secretary of Defense for Intelligence, the Secretary of Defense may recommend to the President either the removal or the retention of the individual. For uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps, the Director may make a recommendation for removal to the Secretary of Defense.
- (3) Nothing in this subsection shall be construed to limit or otherwise affect the authority of the President to nominate, appoint, assign, or terminate the appointment or assignment of any individual, with or without a consultation, recommendation, or concurrence.

1.4 The Intelligence Community

Consistent with applicable Federal law and with the other provisions of this order, and under the leadership of the Director, as specified in such law and this order, the Intelligence Community shall:

- (a) Collect and provide information needed by the President and, in the performance of executive functions, the Vice President, the NSC, the Homeland Security Council, the Chairman of the Joint Chiefs of Staff, senior military commanders, and other executive branch officials and, as appropriate, the Congress of the United States;
- (b) In accordance with priorities set by the President, collect information concerning, and conduct activities to protect against, international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;

- (c) Analyze, produce, and disseminate intelligence;
- (d) Conduct administrative, technical, and other support activities within the United States and abroad necessary for the performance of authorized activities, to include providing services of common concern for the Intelligence Community as designated by the Director in accordance with this order;
- (e) Conduct research, development, and procurement of technical systems and devices relating to authorized functions and missions or the provision of services of common concern for the Intelligence Community;
- (f) Protect the security of intelligence related activities, information, installations, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Intelligence Community elements as are necessary;
- (g) Take into account State, local, and tribal governments' and, as appropriate, private sector entities' information needs relating to national and homeland security;
- (h) Deconflict, coordinate, and integrate all intelligence activities and other information gathering in accordance with section 1.3(b)(20) of this order; and
- (i) Perform such other functions and duties related to intelligence activities as the President may direct.

1.5 Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies

The heads of all departments and agencies shall:

- (a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;
- (b) Provide all programmatic and budgetary information necessary to support the Director in developing the National Intelligence Program;
- (c) Coordinate development and implementation of intelligence systems and architectures and, as appropriate, operational systems and architectures of their departments, agencies, and other elements with the Director to respond to national intelligence requirements and all applicable information sharing and security guidelines, information privacy, and other legal requirements;
- (d) Provide, to the maximum extent permitted by law, subject to the availability of appropriations and not inconsistent with the mission of the department or agency, such further support to the Director as the Director may request, after consultation with the head of the department or agency, for the performance of the Director's functions;

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

1.6 Heads of Elements of the Intelligence Community

The heads of elements of the Intelligence Community shall:

- (a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;
- (b) Report to the Attorney General possible violations of Federal criminal laws by employees and of specified Federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department, agency, or establishment concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;
- (c) Report to the Intelligence Oversight Board, consistent with Executive Order 13462 of February 29, 2008 [note to this section], and provide copies of all such reports to the Director, concerning any intelligence

activities of their elements that they have reason to believe may be unlawful or contrary to executive order or presidential directive;

- (d) Protect intelligence and intelligence sources, methods, and activities from unauthorized disclosure in accordance with guidance from the Director;
- (e) Facilitate, as appropriate, the sharing of information or intelligence, as directed by law or the President, to State, local, tribal, and private sector entities;
- (f) Disseminate information or intelligence to foreign governments and international organizations under intelligence or counterintelligence arrangements or agreements established in accordance with section 1.3(b)(4) of this order;
- (g) Participate in the development of procedures approved by the Attorney General governing production and dissemination of information or intelligence resulting from criminal drug intelligence activities abroad if they have intelligence responsibilities for foreign or domestic criminal drug production and trafficking; and
- (h) Ensure that the inspectors general, general counsels, and agency officials responsible for privacy or civil liberties protection for their respective organizations have access to any information or intelligence necessary to perform their official duties.

1.7 Intelligence Community Elements

Each element of the Intelligence Community shall have the duties and responsibilities specified below, in addition to those specified by law or elsewhere in this order. Intelligence Community elements within executive departments shall serve the information and intelligence needs of their respective heads of departments and also shall operate as part of an integrated Intelligence Community, as provided in law or this order.

(a) THE CENTRAL INTELLIGENCE AGENCY

The Director of the Central Intelligence Agency shall:

- (1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence;
- (2) Conduct counterintelligence activities without assuming or performing any internal security functions within the United States;
- (3) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;
- (4) Conduct covert action activities approved by the President. No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert

action activity unless the President determines that another agency is more likely to achieve a particular objective;

- (5) Conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations consistent with section 1.3(b)(4) of this order;
- (6) Under the direction and guidance of the Director, and in accordance with section 1.3(b)(4) of this order, coordinate the implementation of intelligence and counterintelligence relationships between elements of the Intelligence Community and the intelligence or security services of foreign governments or international organizations; and
- (7) Perform such other functions and duties related to intelligence as the Director may direct.

(b) THE DEFENSE INTELLIGENCE AGENCY

The Director of the Defense Intelligence Agency shall:

- (1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions;
- (2) Collect, analyze, produce, or, through tasking and coordination, provide defense and defense-related intelligence for the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, combatant commanders, other Defense components, and non-Defense agencies;
- (3) Conduct counterintelligence activities;
- (4) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;
- (5) Conduct foreign defense intelligence liaison relationships and defense intelligence exchange programs with foreign defense establishments, intelligence or security services of foreign governments, and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order;
- (6) Manage and coordinate all matters related to the Defense Attaché system; and
- (7) Provide foreign intelligence and counterintelligence staff support as directed by the Secretary of Defense.

(c) THE NATIONAL SECURITY AGENCY

The Director of the National Security Agency shall:

- (1) Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;
- (2) Establish and operate an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the

Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director;

- (3) Control signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders;
- (4) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements;
- (5) Provide signals intelligence support for national and departmental requirements and for the conduct of military operations;
- (6) Act as the National Manager for National Security Systems as established in law and policy, and in this capacity be responsible to the Secretary of Defense and to the Director;
- (7) Prescribe, consistent with section 102A(g) of the Act [50 U.S.C. § 403-1(g)], within its field of authorized operations, security regulations covering operating practices, including the transmission, handling, and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the National Security Agency, and exercise the necessary supervisory control to ensure compliance with the regulations; and
- (8) Conduct foreign cryptologic liaison relationships in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(d) THE NATIONAL RECONNAISSANCE OFFICE

The Director of the National Reconnaissance Office shall:

- (1) Be responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States Government needs; and
- (2) Conduct foreign liaison relationships relating to the above missions, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(e) THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

The Director of the National Geospatial-Intelligence Agency shall:

- (1) Collect, process, analyze, produce, and disseminate geospatial intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;
- (2) Provide geospatial intelligence support for national and departmental requirements and for the conduct of military operations;
- (3) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements; and
- (4) Conduct foreign geospatial intelligence liaison relationships, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(f) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE ARMY, NAVY, AIR FORCE, AND MARINE CORPS

The Commanders and heads of the intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps shall:

- (1) Collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements;
- (2) Conduct counterintelligence activities;
- (3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and
- (4) Conduct military intelligence liaison relationships and military intelligence exchange programs with selected cooperative foreign defense establishments and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(g) INTELLIGENCE ELEMENTS OF THE FEDERAL BUREAU OF INVESTIGATION

Under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the intelligence elements of the Federal Bureau of Investigation shall:

- (1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions, in accordance with procedural guidelines approved by the Attorney General, after consultation with the Director;
- (2) Conduct counterintelligence activities; and
- (3) Conduct foreign intelligence and counterintelligence liaison relationships with intelligence, security, and law enforcement services of foreign governments or international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(h) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE COAST GUARD

The Commandant of the Coast Guard shall:

- (1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence including defense and defense-related information and intelligence to support national and departmental missions;
- (2) Conduct counterintelligence activities;

- (3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and
- (4) Conduct foreign intelligence liaison relationships and intelligence exchange programs with foreign intelligence services, security services or international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and, when operating as part of the Department of Defense, 1.10(i) of this order.

(i) THE BUREAU OF INTELLIGENCE AND RESEARCH, DEPARTMENT OF STATE; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF THE TREASURY; THE OFFICE OF NATIONAL SECURITY INTELLIGENCE, DRUG ENFORCEMENT ADMINISTRATION; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY; AND THE OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE, DEPARTMENT OF ENERGY

The heads of the Bureau of Intelligence and Research, Department of State; the Office of Intelligence and Analysis, Department of the Treasury; the Office of National Security Intelligence, Drug Enforcement Administration; the Office of Intelligence and Analysis, Department of Homeland Security; and the Office of Intelligence and Counterintelligence, Department of Energy shall:

- (1) Collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions; and
- (2) Conduct and participate in analytic or information exchanges with foreign partners and international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(j) THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

The Director shall collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support the missions of the Office of the Director of National Intelligence, including the National Counterterrorism Center, and to support other national missions.

1.8 The Department of State

In addition to the authorities exercised by the Bureau of Intelligence and Research under sections 1.4 and 1.7(i) of this order, the Secretary of State shall:

- (a) Collect (overtly or through publicly available sources) information relevant to United States foreign policy and national security concerns;
- (b) Disseminate, to the maximum extent possible, reports received from United States diplomatic and consular posts;

- (c) Transmit reporting requirements and advisory taskings of the Intelligence Community to the Chiefs of United States Missions abroad; and
- (d) Support Chiefs of United States Missions in discharging their responsibilities pursuant to law and presidential direction.

1.9 The Department of the Treasury

In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of the Treasury under sections 1.4 and 1.7(i) of this order the Secretary of the Treasury shall collect (overtly or through publicly available sources) foreign financial information and, in consultation with the Department of State, foreign economic information.

1.10 The Department of Defense

The Secretary of Defense shall:

- (a) Collect (including through clandestine means), analyze, produce, and disseminate information and intelligence and be responsive to collection tasking and advisory tasking by the Director;
- (b) Collect (including through clandestine means), analyze, produce, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution of the Secretary's responsibilities;
- (c) Conduct programs and missions necessary to fulfill national, departmental, and tactical intelligence requirements;
- (d) Conduct counterintelligence activities in support of Department of Defense components and coordinate counterintelligence activities in accordance with section 1.3(b)(20) and (21) of this order;
- (e) Act, in coordination with the Director, as the executive agent of the United States Government for signals intelligence activities;
- (f) Provide for the timely transmission of critical intelligence, as defined by the Director, within the United States Government;
- (g) Carry out or contract for research, development, and procurement of technical systems and devices relating to authorized intelligence functions;
- (h) Protect the security of Department of Defense installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Department of Defense as are necessary;
- (i) Establish and maintain defense intelligence relationships and defense intelligence exchange programs with selected cooperative foreign defense establishments, intelligence or security services of foreign governments, and international organizations, and ensure that such relationships and programs are in accordance with sections 1.3(b)(4), 1.3(b)(21) and 1.7(a)(6) of this order;

- (j) Conduct such administrative and technical support activities within and outside the United States as are necessary to provide for cover and proprietary arrangements, to perform the functions described in sections (a) though (i) above, and to support the Intelligence Community elements of the Department of Defense; and
- (k) Use the Intelligence Community elements within the Department of Defense identified in section 1.7(b) through (f) and, when the Coast Guard is operating as part of the Department of Defense, (h) above to carry out the Secretary of Defense's responsibilities assigned in this section or other departments, agencies, or offices within the Department of Defense, as appropriate, to conduct the intelligence missions and responsibilities assigned to the Secretary of Defense.

1.11 The Department of Homeland Security

In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of Homeland Security under sections 1.4 and 1.7(i) of this order, the Secretary of Homeland Security shall conduct, through the United States Secret Service, activities to determine the existence and capability of surveillance equipment being used against the President or the Vice President of the United States, the Executive Office of the President, and, as authorized by the Secretary of Homeland Security or the President, other Secret Service protectees and United States officials. No information shall be acquired intentionally through such activities except to protect against use of such surveillance equipment, and those activities shall be conducted pursuant to procedures agreed upon by the Secretary of Homeland Security and the Attorney General.

1.12 The Department of Energy

In addition to the authorities exercised by the Office of Intelligence and Counterintelligence of the Department of Energy under sections 1.4 and 1.7(i) of this order, the Secretary of Energy shall:

- (a) Provide expert scientific, technical, analytic, and research capabilities to other agencies within the Intelligence Community, as appropriate;
- (b) Participate in formulating intelligence collection and analysis requirements where the special expert capability of the Department can contribute; and
- (c) Participate with the Department of State in overtly collecting information with respect to foreign energy matters.

1.13 The Federal Bureau of Investigation

In addition to the authorities exercised by the intelligence elements of the Federal Bureau of Investigation of the Department of Justice under sections 1.4 and 1.7(g) of this order and under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the Director of the Federal Bureau of Investigation shall provide technical assistance, within or outside the United States, to foreign intelligence and law enforcement services,

consistent with section 1.3(b)(20) and (21) of this order, as may be necessary to support national or departmental missions.

Part 2: Conduct of Intelligence Activities

2.1 Need

Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to informed decisionmaking in the areas of national security, national defense, and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.

2.2 Purpose

This Order is intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities, the spread of weapons of mass destruction, and espionage conducted by foreign powers. Set forth below are certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests. Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency.

2.3 Collection of Information

Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director. Those procedures shall permit collection, retention, and dissemination of the following types of information:

- (a) Information that is publicly available or collected with the consent of the person concerned;
- (b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for

the purpose of acquiring information concerning the domestic activities of United States persons;

- (c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drugs, or international terrorism investigation;
- (d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;
- (e) Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other elements of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting;
- (f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;
- (g) Information arising out of a lawful personnel, physical, or communications security investigation;
- (h) Information acquired by overhead reconnaissance not directed at specific United States persons;
- (i) Incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws; and
- (j) Information necessary for administrative purposes.

In addition, elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the Director in coordination with the Secretary of Defense and approved by the Attorney General.

2.4 Collection Techniques

Elements of the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Elements of the Intelligence Community are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element concerned and approved by the Attorney General, after consultation with the Director. Such procedures shall protect constitutional and other legal rights

and limit use of such information to lawful governmental purposes. These procedures shall not authorize:

- (a) The Central Intelligence Agency (CIA) to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance;
- (b) Unconsented physical searches in the United States by elements of the Intelligence Community other than the FBI, except for:
    - (1) Searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes, when authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers; and
    - (2) Searches by CIA of personal property of non-United States persons lawfully in its possession;
- (c) Physical surveillance of a United States person in the United States by elements of the Intelligence Community other than the FBI, except for:
    - (1) Physical surveillance of present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting; and
    - (2) Physical surveillance of a military person employed by a nonintelligence element of a military service; and
- (d) Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.

2.5 Attorney General Approval

The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. The authority delegated pursuant to this paragraph, including the authority to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978 [50 U.S.C. §§ 1801 et seq.], as amended, shall be exercised in accordance with that Act.

2.6 Assistance to Law Enforcement and other Civil Authorities

Elements of the Intelligence Community are authorized to:

- (a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property, and facilities of any element within the Intelligence Community;

- (b) Unless otherwise precluded by law or this Order, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities;
- (c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or, when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the general counsel of the providing element or department; and
- (d) Render any other assistance and cooperation to law enforcement or other civil authorities not precluded by applicable law.

2.7 Contracting

Elements of the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contracts or arrangements for authorized intelligence purposes. Contracts or arrangements with academic institutions may be undertaken only with the consent of appropriate officials of the institution.

2.8 Consistency with Other Laws

Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.

2.9 Undisclosed Participation in Organizations within the United States

No one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without disclosing such person's intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the Intelligence Community element head or designee. No such participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where:

- (a) The participation is undertaken on behalf of the FBI in the course of a lawful investigation; or
- (b) The organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power.

2.10 Human Experimentation

No element of the Intelligence Community shall sponsor, contract for, or conduct research on human subjects except in accordance with guidelines issued by the Department of Health and Human Services. The subject's informed consent shall be documented as required by those guidelines.

2.11 Prohibition on Assassination

No person employed by or acting on behalf of the United States Government shall engage in, or conspire to engage in, assassination.

2.12 Indirect Participation

No element of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order.

2.13 Limitation on Covert Action

No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.

Part 3: General Provisions

3.1 Congressional Oversight

The duties and responsibilities of the Director and the heads of other departments, elements, and entities engaged in intelligence activities to cooperate with the Congress in the conduct of its responsibilities for oversight of intelligence activities shall be implemented in accordance with applicable law, including title V of the Act [50 U.S.C. §§ 413 et seq.]. The requirements of applicable law, including title V of the Act [50 U.S.C. §§ 413 et seq.], shall apply to all covert action activities as defined in this Order.

3.2 Implementation

The President, supported by the NSC, and the Director shall issue such appropriate directives, procedures, and guidance as are necessary to implement this order. Heads of elements within the Intelligence Community shall issue appropriate procedures and supplementary directives consistent with this order. No procedures to implement Part 2 of this order shall be issued without the Attorney General's approval, after consultation with the Director. The Attorney General shall provide a statement of reasons for not approving any procedures established by the head of an element in the Intelligence Community (or the head of the department containing such element) other than the FBI. In instances where the element head or department head and the Attorney General are unable to reach agreements on other than constitutional or other legal grounds, the Attorney General, the head of department concerned, or the Director shall refer the matter to the NSC.

3.3 Procedures

The activities herein authorized that require procedures shall be conducted in accordance with existing procedures or requirements established under Executive Order 12333 [this note]. New procedures, as required by Executive Order 12333, as further amended, shall be established as expeditiously as possible. All new procedures promulgated pursuant to Executive Order 12333, as amended, shall be made available to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

3.4 References and Transition

References to 'Senior Officials of the Intelligence Community' or 'SOICs' in executive orders or other Presidential guidance, shall be deemed references to the heads of elements in the Intelligence Community, unless the President otherwise directs; references in Intelligence Community or Intelligence Community element policies or guidance, shall be deemed to be references to the heads of elements of the Intelligence Community, unless the President or the Director otherwise directs.

3.5 Definitions

For the purposes of this Order, the following terms shall have these meanings:

- (a) Counterintelligence means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities.
- (b) Covert action means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include:
    - (1) Activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;
    - (2) Traditional diplomatic or military activities or routine support to such activities;
    - (3) Traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or
    - (4) Activities to provide routine support to the overt activities (other than activities described in paragraph (1), (2), or (3)) of other United States Government agencies abroad.
- (c) Electronic surveillance means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic

communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

- (d) Employee means a person employed by, assigned or detailed to, or acting for an element within the Intelligence Community.
- (e) Foreign intelligence means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.
- (f) Intelligence includes foreign intelligence and counterintelligence.
- (g) Intelligence activities means all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.
- (h) Intelligence Community and elements of the Intelligence Community refers to:
    - (1) The Office of the Director of National Intelligence;
    - (2) The Central Intelligence Agency;
    - (3) The National Security Agency;
    - (4) The Defense Intelligence Agency;
    - (5) The National Geospatial-Intelligence Agency;
    - (6) The National Reconnaissance Office;
    - (7) The other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;
    - (8) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;
    - (9) The intelligence elements of the Federal Bureau of Investigation;
    - (10) The Office of National Security Intelligence of the Drug Enforcement Administration;
    - (11) The Office of Intelligence and Counterintelligence of the Department of Energy;
    - (12) The Bureau of Intelligence and Research of the Department of State;
    - (13) The Office of Intelligence and Analysis of the Department of the Treasury;
    - (14) The Office of Intelligence and Analysis of the Department of Homeland Security;
    - (15) The intelligence and counterintelligence elements of the Coast Guard; and
    - (16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community.
- (i) National Intelligence and Intelligence Related to National Security means all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that

pertains, as determined consistent with any guidance issued by the President, or that is determined for the purpose of access to information by the Director in accordance with section 1.3(a)(1) of this order, to pertain to more than one United States Government agency; and that involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security.

- (j) The National Intelligence Program means all programs, projects, and activities of the Intelligence Community, as well as any other programs of the Intelligence Community designated jointly by the Director and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.
- (k) United States person means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

3.6 Revocation

Executive Orders 13354 [50 U.S.C. § 4040] and 13355 of August 27, 2004 [50 U.S.C. § 403-4a note], are revoked; and paragraphs 1.3(b)(9) and (10) of Part 1 supersede provisions within Executive Order 12958 [50 U.S.C. § 435 note], as amended, to the extent such provisions in Executive Order 12958 [50 U.S.C. § 435 note], as amended, are inconsistent with this Order.

3.7 General Provisions

- (a) Consistent with section 1.3(c) of this order, nothing in this order shall be construed to impair or otherwise affect:
    - (1) Authority granted by law to a department or agency, or the head thereof; or
    - (2) Functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.
- (b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.
- (c) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person.

Executive Order 12,949: Foreign Intelligence Physical Searches

As Amended Through January 1, 2010

Exec. Order No. 12,949, Foreign *Intelligence Physical Searches*, 60 Fed. Reg. 8169 (Feb. 9, 1995); Exec. Order No. 13383, 70 Fed. Reg. 41933 (July 15, 2005); Exec. Order No. 13475, 73 Fed. Reg. 60095 (October 7, 2008), *available at* http://www.intelligencelaw.com/library/admin/html/eo_12949_2010.html.

Exec. Order No. 12,949, Foreign Intelligence Physical Searches, provides:

By the authority vested in me as President by the Constitution and the laws of the United States, including sections 302 and 303 of the Foreign Intelligence Surveillance Act of 1978 ('Act') (50 U.S.C. 1801, et seq.) [50 U.S.C. §§ 1822, 1823], as amended by Public Law 103-359, and in order to provide for the authorization of physical searches for foreign intelligence purposes as set forth in the Act, it is hereby ordered as follows:

Section 1

Pursuant to section 302(a)(1) of the Act [50 U.S.C. § 1822(a)(1)], the Attorney General is authorized to approve physical searches, without a court order, to acquire foreign intelligence information for periods of up to one year, if the Attorney General makes the certifications required by that section.

Section 2

Pursuant to section 302(b) of the Act [50 U.S.C. § 1822(b)], the Attorney General is authorized to approve applications to the Foreign Intelligence Surveillance Court under section 303 of the Act to obtain orders for physical searches for the purpose of collecting foreign intelligence information.

Section 3

Pursuant to section 303(a)(6) of the Act [50 U.S.C. § 1823(a)(6)], the following officials, each of whom is employed in the area of national security or defense, is designated to make the certifications required by section 303(a)(6) of the Act [50 U.S.C. § 1823(a)(6)] in support of applications to conduct physical searches:

- (a) Secretary of State;
- (b) Secretary of Defense;
- (c) Director of National Intelligence;
- (d) Director of the Federal Bureau of Investigation;
- (e) Deputy Secretary of State;
- (f) Deputy Secretary of Defense;
- (g) Director of the Central Intelligence Agency;
- (h) Principal Deputy Director of National Intelligence; and

- (i) Deputy Director of the Federal Bureau of Investigation.

None of the above officials, nor anyone officially acting in that capacity, may exercise the authority to make the above certifications, unless that official has been appointed by the President, by and with the advice and consent of the Senate. The requirement of the preceding sentence that the named official must be appointed by the President with the advice and consent of the Senate does not apply to the Deputy Director of the Federal Bureau of Investigation.

Executive Order 13,526: Classified National Security Information

As Amended Through January 1, 2010

Exec. Order No. 13,526, *Classified National Security Information* (December 29, 2009), *available at* http://www.intelligencelaw.com/library/admin/html/eo_13526_12-29-2009.html.

Table of Contents

Preamble

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

NOW, THEREFORE, I, BARACK OBAMA, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Part 1—Original Classification

Sec. 1.1. Classification Standards

(a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

(1) an original classification authority is classifying the information;

(2) the information is owned by, produced by or for, or is under the control of the United States Government;

(3) the information falls within one or more of the categories of information listed in section 1.4 of this order; and

(4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

(d) The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.

Sec. 1.2. Classification Levels

(a) Information may be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

Sec. 1.3. Classification Authority

(a) The authority to classify information originally may be exercised only by:

(1) the President and the Vice President;

(2) agency heads and officials designated by the President; and

(3) United States Government officials delegated this authority pursuant to paragraph (c) of this section.

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) Delegation of original classification authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) "Top Secret" original classification authority may be delegated only by the President, the Vice President, or an agency head or official designated pursuant to paragraph (a)(2) of this section.

(3) "Secret" or "Confidential" original classification authority may be delegated only by the President, the Vice President, an agency head or official designated pursuant to paragraph (a)(2) of this section, or the senior agency official designated under section 5.4(d) of this order, provided that official has been delegated "Top Secret" original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position.

(5) Delegations of original classification authority shall be reported or made available by name or position to the Director of the Information Security Oversight Office.

(d) All original classification authorities must receive training in proper classification (including the avoidance of over-classification) and declassification as provided in this order and its implementing directives at least once a calendar year. Such training must include instruction on the proper safeguarding of classified information and on the sanctions in section 5.5 of this order that may be brought against an individual who fails to classify information properly or protect classified information from unauthorized disclosure. Original classification authorities who do not receive such mandatory training at least once within a calendar year shall have their classification authority suspended by the agency head or the senior agency official designated under section 5.4(d) of this order until such training has taken place. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

(e) Exceptional cases. When an employee, government contractor, licensee, certificate holder, or grantee of an agency who does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority

with respect to this information. That agency shall decide within 30 days whether to classify this information.

Sec. 1.4. Classification Categories

Information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 1.2 of this order, and it pertains to one or more of the following:

(a) military plans, weapons systems, or operations;

(b) foreign government information;

(c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;

(d) foreign relations or foreign activities of the United States, including confidential sources;

(e) scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities;

(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or

(h) the development, production, or use of weapons of mass destruction.

Sec. 1.5. Duration of Classification

(a) At the time of original classification, the original classification authority shall establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. Except for information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, the date or event shall not exceed the time frame established in paragraph (b) of this section.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it be marked for declassification for up to 25 years from the date of the original decision.

(c) An original classification authority may extend the duration of classification up to 25 years from the date of origin of the document, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this order are followed.

(d) No information may remain classified indefinitely. Information marked for an indefinite duration of classification under predecessor orders, for example, marked as "Originating Agency's Determination Required," or classified information that contains incomplete declassification instructions or lacks declassification instructions shall be declassified in accordance with part 3 of this order.

Sec. 1.6. Identification and Markings

(a) At the time of original classification, the following shall be indicated in a manner that is immediately apparent:

(1) one of the three classification levels defined in section 1.2 of this order;

(2) the identity, by name and position, or by personal identifier, of the original classification authority;

(3) the agency and office of origin, if not otherwise evident;

(4) declassification instructions, which shall indicate one of the following:

(A) the date or event for declassification, as prescribed in section 1.5(a);

(B) the date that is 10 years from the date of original classification, as prescribed in section 1.5(b);

(C) the date that is up to 25 years from the date of original classification, as prescribed in section 1.5(b); or

(D) in the case of information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, the marking prescribed in implementing directives issued pursuant to this order; and

(5) a concise reason for classification that, at a minimum, cites the applicable classification categories in section 1.4 of this order.

(b) Specific information required in paragraph (a) of this section may be excluded if it would reveal additional classified information.

(c) With respect to each classified document, the agency originating the document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant and revoke temporary waivers of this requirement. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings or other indicia implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking provided that the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form.

(h) Prior to public release, all declassified records shall be appropriately marked to reflect their declassification.

Sec. 1.7. Classification Prohibitions and Limitations

(a) In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:

(1) conceal violations of law, inefficiency, or administrative error;

(2) prevent embarrassment to a person, organization, or agency;

(3) restrain competition; or

(4) prevent or delay the release of information that does not require protection in the interest of the national security.

(b) Basic scientific research information not clearly related to the national security shall not be classified.

(c) Information may not be reclassified after declassification and release to the public under proper authority unless:

(1) the reclassification is personally approved in writing by the agency head based on a document-by-document determination by the agency that reclassification is required to prevent significant and demonstrable damage to the national security;

(2) the information may be reasonably recovered without bringing undue attention to the information;

(3) the reclassification action is reported promptly to the Assistant to the President for National Security Affairs (National Security Advisor) and the Director of the Information Security Oversight Office; and

(4) for documents in the physical and legal custody of the National Archives and Records Administration (National Archives) that have been available for public use, the agency head has, after making the determinations required by this paragraph, notified the Archivist of the United States (Archivist), who shall suspend public access pending approval of the reclassification action by the Director of the Information Security Oversight Office. Any such decision by the Director may be appealed by the agency head to the President through the National Security Advisor. Public access shall remain suspended pending a prompt decision on the appeal.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552), the Presidential Records Act, 44 U.S.C. 2204(c)(1), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.5 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.4 of this order. The requirements in this paragraph also apply to those situations in which information has been declassified in accordance with a specific date or event determined by an original classification authority in accordance with section 1.5 of this order.

(e) Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or

relationship that: (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information.

Sec. 1.8. Classification Challenges

(a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b) of this section.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information, including authorized holders outside the classifying agency, are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall ensure that:

(1) individuals are not subject to retribution for bringing such actions;

(2) an opportunity is provided for review by an impartial official or panel; and

(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel (Panel) established by section 5.3 of this order.

(c) Documents required to be submitted for prepublication review or other administrative process pursuant to an approved nondisclosure agreement are not covered by this section.

Sec. 1.9. Fundamental Classification Guidance Review

(a) Agency heads shall complete on a periodic basis a comprehensive review of the agency's classification guidance, particularly classification guides, to ensure the guidance reflects current circumstances and to identify classified information that no longer requires protection and can be declassified. The initial fundamental classification guidance review shall be completed within 2 years of the effective date of this order.

(b) The classification guidance review shall include an evaluation of classified information to determine if it meets the standards for classification under section 1.4 of this order, taking into account an up-to-date assessment of likely damage as described under section 1.2 of this order.

(c) The classification guidance review shall include original classification authorities and agency subject matter experts to ensure a broad range of perspectives.

(d) Agency heads shall provide a report summarizing the results of the classification guidance review to the Director of the Information Security Oversight Office and shall release an unclassified version of this report to the public.

Part 2—Derivative Classification

Sec. 2.1. Use of Derivative Classification

(a) Persons who reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:
(1) be identified by name and position, or by personal identifier, in a manner that is immediately apparent for each derivative classification action;

(2) observe and respect original classification decisions; and

(3) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(A) the date or event for declassification that corresponds to the longest period of classification among the sources, or the marking established pursuant to section 1.6(a)(4)(D) of this order; and

(B) a listing of the source materials.

(c) Derivative classifiers shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form.

(d) Persons who apply derivative classification markings shall receive training in the proper application of the derivative classification principles of the order, with an emphasis on avoiding over-classification, at least once every 2 years. Derivative classifiers who do not receive such training at least once every 2 years shall have their authority to apply derivative classification markings suspended until they have received such training. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

Sec. 2.2. Classification Guides

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official; and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to ensure that classification guides are reviewed and updated as provided in directives issued under this order.

(d) Agencies shall incorporate original classification decisions into classification guides on a timely basis and in accordance with directives issued under this order.

(e) Agencies may incorporate exemptions from automatic declassification approved pursuant to section 3.3(j) of this order into classification guides, provided that the Panel is notified of the intent to take such action for specific information in advance of approval and the information remains in active use.

(f) The duration of classification of a document classified by a derivative classifier using a classification guide shall not exceed 25 years from the date of the origin of the document, except for:

(1) information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction; and

(2) specific information incorporated into classification guides in accordance with section 2.2(e) of this order.

Part 3—Declassification and Downgrading

Sec. 3.1. Authority for Declassification

(a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) Information shall be declassified or downgraded by:

(1) the official who authorized the original classification, if that official is still serving in the same position and has original classification authority;

(2) the originator's current successor in function, if that individual has original classification authority;

(3) a supervisory official of either the originator or his or her successor in function, if the supervisory official has original classification authority; or

(4) officials delegated declassification authority in writing by the agency head or the senior agency official of the originating agency.

(c) The Director of National Intelligence (or, if delegated by the Director of National Intelligence, the Principal Deputy Director of National Intelligence) may, with respect to the Intelligence Community, after consultation with the head of the originating Intelligence Community element or department, declassify, downgrade, or direct the declassification or downgrading of information or intelligence relating to intelligence sources, methods, or activities.

(d) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(e) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the National Security Advisor. The information shall remain classified pending a prompt decision on the appeal.

(f) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

(g) No information may be excluded from declassification under section 3.3 of this order based solely on the type of document or record in which it is found. Rather, the classified information must be considered on the basis of its content.

(h) Classified nonrecord materials, including artifacts, shall be declassified as soon as they no longer meet the standards for classification under this order.

(i) When making decisions under sections 3.3, 3.4, and 3.5 of this order, agencies shall consider the final decisions of the Panel.

Sec. 3.2. Transferred Records

(a) In the case of classified records transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified records that are not officially transferred as described in paragraph (a) of this section, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such records shall be deemed to be the originating agency for purposes of this order. Such records may be declassified or downgraded by the agency in possession of the records after consultation with any other agency that has an interest in the subject matter of the records.

(c) Classified records accessioned into the National Archives shall be declassified or downgraded by the Archivist in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that classified records be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to records transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or records for which the National Archives serves as the custodian of the records of an agency or organization that has gone out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in section 3.3 of this order.

Sec. 3.3. Automatic Declassification

(a) Subject to paragraphs (b)–(d) and (g)–(j) of this section, all classified records that (1) are more than 25 years old and (2) have been determined to have

permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. All classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of origin, except as provided in paragraphs (b)–(d) and (g)–(i) of this section. If the date of origin of an individual record cannot be readily determined, the date of original classification shall be used instead.

(b) An agency head may exempt from automatic declassification under paragraph (a) of this section specific information, the release of which should clearly and demonstrably be expected to:

(1) reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development;

(2) reveal information that would assist in the development, production, or use of weapons of mass destruction;

(3) reveal information that would impair U.S. cryptologic systems or activities;

(4) reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;

(5) reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;

(6) reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States;

(7) reveal information that would impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

(8) reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security; or

(9) violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

(c)(1) An agency head shall notify the Panel of any specific file series of records for which a review or assessment has determined that the information within that file series almost invariably falls within one or more of the exemption categories listed in paragraph (b) of this section and that the agency proposes to exempt from automatic declassification at 25 years.

(2) The notification shall include:

(A) a description of the file series;

(B) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and

(C) except when the information within the file series almost invariably identifies a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, a specific date or event for declassification of the information, not to exceed December 31 of the year that is 50 years from the date of origin of the records.

(3) The Panel may direct the agency not to exempt a designated file series or to declassify the information within that series at an earlier date than recommended. The agency head may appeal such a decision to the President through the National Security Advisor.

(4) File series exemptions approved by the President prior to December 31, 2008, shall remain valid without any additional agency action pending Panel review by the later of December 31, 2010, or December 31 of the year that is 10 years from the date of previous approval.

(d) The following provisions shall apply to the onset of automatic declassification:

(1) Classified records within an integral file block, as defined in this order, that are otherwise subject to automatic declassification under this section shall not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block.

(2) After consultation with the Director of the National Declassification Center (the Center) established by section 3.7 of this order and before the records are subject to automatic declassification, an agency head or senior agency official may delay automatic declassification for up to five additional years for classified information contained in media that make a review for possible declassification exemptions more difficult or costly.

(3) Other than for records that are properly exempted from automatic declassification, records containing classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies with respect to the classified information and could reasonably be expected to fall under one or more of the exemptions in paragraph (b) of this section shall be identified prior to the onset of automatic declassification for later referral to those agencies.

(A) The information of concern shall be referred by the Center established by section 3.7 of this order, or by the centralized facilities referred to in section 3.7(e) of this order, in a prioritized and scheduled manner determined by the Center.

(B) If an agency fails to provide a final determination on a referral made by the Center within 1 year of referral, or by the centralized facilities referred to in section 3.7(e) of this order within 3 years of referral, its equities in the referred records shall be automatically declassified.

(C) If any disagreement arises between affected agencies and the Center regarding the referral review period, the Director of the Information Security Oversight Office shall determine the appropriate period of review of referred records.

(D) Referrals identified prior to the establishment of the Center by section 3.7 of this order shall be subject to automatic declassification only in accordance with subparagraphs (d)(3)(A)–(C) of this section.

(4) After consultation with the Director of the Information Security Oversight Office, an agency head may delay automatic declassification for up to 3 years from the date of discovery of classified records that were inadvertently not reviewed prior to the effective date of automatic declassification.

(e) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

(f) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

(g) The Secretary of Energy shall determine when information concerning foreign nuclear programs that was removed from the Restricted Data category in order to carry out provisions of the National Security Act of 1947, as amended, may be declassified. Unless otherwise determined, such information shall be declassified when comparable information concerning the United States nuclear program is declassified.

(h) Not later than 3 years from the effective date of this order, all records exempted from automatic declassification under paragraphs (b) and (c) of this section shall be automatically declassified on December 31 of a year that is no more than 50 years from the date of origin, subject to the following:

(1) Records that contain information the release of which should clearly and demonstrably be expected to reveal the following are exempt from automatic declassification at 50 years:

(A) the identity of a confidential human source or a human intelligence source; or

(B) key design concepts of weapons of mass destruction.

(2) In extraordinary cases, agency heads may, within 5 years of the onset of automatic declassification, propose to exempt additional specific information from declassification at 50 years.

(3) Records exempted from automatic declassification under this paragraph shall be automatically declassified on December 31 of a year that is no more than 75 years from the date of origin unless an agency head, within 5 years of that date, proposes to exempt specific information from declassification at 75 years and the proposal is formally approved by the Panel.

(i) Specific records exempted from automatic declassification prior to the establishment of the Center described in section 3.7 of this order shall be subject to the provisions of paragraph (h) of this section in a scheduled and prioritized manner determined by the Center.

(j) At least 1 year before information is subject to automatic declassification under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Panel, of any specific information that the agency proposes to exempt from automatic declassification under paragraphs (b) and (h) of this section.

(1) The notification shall include:

(A) a detailed description of the information, either by reference to information in specific records or in the form of a declassification guide;

(B) an explanation of why the information should be exempt from automatic declassification and must remain classified for a longer period of time; and

(C) a specific date or a specific and independently verifiable event for automatic declassification of specific records that contain the information proposed for exemption.

(2) The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. An agency head may appeal such a decision to the President through the National Security Advisor. The information will remain classified while such an appeal is pending.

(k) For information in a file series of records determined not to have permanent historical value, the duration of classification beyond 25 years shall be the same as the disposition (destruction) date of those records in each Agency Records Control Schedule or General Records Schedule, although the duration of classification shall be extended if the record has been retained for business reasons beyond the scheduled disposition date.

Sec. 3.4. Systematic Declassification Review

(a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review for records of permanent historical value exempted from automatic declassification under section 3.3 of this order. Agencies shall prioritize their review of such records in accordance with priorities established by the Center.

(b) The Archivist shall conduct a systematic declassification review program for classified records: (1) accessioned into the National Archives; (2) transferred to the Archivist pursuant to 44 U.S.C. 2203; and (3) for which the National Archives serves as the custodian for an agency or organization that has gone out of existence.

Sec. 3.5. Mandatory Declassification Review

(a) Except as provided in paragraph (b) of this section, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

(1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

(2) the document or material containing the information responsive to the request is not contained within an operational file exempted from search and review, publication, and disclosure under 5 U.S.C. 552 in accordance with law; and

(3) the information is not the subject of pending litigation.

(b) Information originated by the incumbent President or the incumbent Vice President; the incumbent President's White House Staff or the incumbent Vice President's Staff; committees, commissions, or boards appointed by the incumbent President; or other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a) of this section. However, the Archivist shall have the authority to review, downgrade, and declassify papers or records of former Presidents and Vice Presidents under the control of the Archivist pursuant to 44 U.S.C. 2107, 2111, 2111 note, or 2203. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Panel. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) If an agency has reviewed the requested information for declassification within the past 2 years, the agency need not conduct another review and may instead inform the requester of this fact and the prior review decision and advise the requester of appeal rights provided under subsection (e) of this section.

(e) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Panel.

(f) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information; the Director of National Intelligence shall develop special procedures for the review of information pertaining to intelligence sources, methods, and activities; and the

Archivist shall develop special procedures for the review of information accessioned into the National Archives.

(g) Documents required to be submitted for prepublication review or other administrative process pursuant to an approved nondisclosure agreement are not covered by this section.

(h) This section shall not apply to any request for a review made to an element of the Intelligence Community that is made by a person other than an individual as that term is defined by 5 U.S.C. 552a(a)(2), or by a foreign government entity or any representative thereof.

Sec. 3.6. Processing Requests and Reviews

Notwithstanding section 4.1(i) of this order, in response to a request for information under the Freedom of Information Act, the Presidential Records Act, the Privacy Act of 1974, or the mandatory review provisions of this order:

(a) An agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified under this order or its predecessors.

(b) When an agency receives any request for documents in its custody that contain classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies with respect to the classified information, or identifies such documents in the process of implementing sections 3.3 or 3.4 of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order or its predecessors. In cases in which the originating agency determines in writing that a response under paragraph (a) of this section is required, the referring agency shall respond to the requester in accordance with that paragraph.

(c) Agencies may extend the classification of information in records determined not to have permanent historical value or nonrecord materials, including artifacts, beyond the time frames established in sections 1.5(b) and 2.2(f) of this order, provided:

(1) the specific information has been approved pursuant to section 3.3(j) of this order for exemption from automatic declassification; and

(2) the extension does not exceed the date established in section 3.3(j) of this order.

Sec. 3.7. National Declassification Center

(a) There is established within the National Archives a National Declassification Center to streamline declassification processes, facilitate quality-assurance measures, and implement standardized training regarding the declassification of records determined to have permanent historical value. There shall be a Director of the Center who shall be appointed or removed by the Archivist in consultation with the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence.

(b) Under the administration of the Director, the Center shall coordinate:

(1) timely and appropriate processing of referrals in accordance with section 3.3(d)(3) of this order for accessioned Federal records and transferred presidential records.

(2) general interagency declassification activities necessary to fulfill the requirements of sections 3.3 and 3.4 of this order;

(3) the exchange among agencies of detailed declassification guidance to enable the referral of records in accordance with section 3.3(d)(3) of this order;

(4) the development of effective, transparent, and standard declassification work processes, training, and quality assurance measures;

(5) the development of solutions to declassification challenges posed by electronic records, special media, and emerging technologies;

(6) the linkage and effective utilization of existing agency databases and the use of new technologies to document and make public declassification review decisions and support declassification activities under the purview of the Center; and

(7) storage and related services, on a reimbursable basis, for Federal records containing classified national security information.

(c) Agency heads shall fully cooperate with the Archivist in the activities of the Center and shall:

(1) provide the Director with adequate and current declassification guidance to enable the referral of records in accordance with section 3.3(d)(3) of this order; and

(2) upon request of the Archivist, assign agency personnel to the Center who shall be delegated authority by the agency head to review and exempt or declassify information originated by their agency contained in records

accessioned into the National Archives, after consultation with subject-matter experts as necessary.

(d) The Archivist, in consultation with representatives of the participants in the Center and after input from the general public, shall develop priorities for declassification activities under the purview of the Center that take into account the degree of researcher interest and the likelihood of declassification.

(e) Agency heads may establish such centralized facilities and internal operations to conduct internal declassification reviews as appropriate to achieve optimized records management and declassification business processes. Once established, all referral processing of accessioned records shall take place at the Center, and such agency facilities and operations shall be coordinated with the Center to ensure the maximum degree of consistency in policies and procedures that relate to records determined to have permanent historical value.

(f) Agency heads may exempt from automatic declassification or continue the classification of their own originally classified information under section 3.3(a) of this order except that in the case of the Director of National Intelligence, the Director shall also retain such authority with respect to the Intelligence Community.

(g) The Archivist shall, in consultation with the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, the Director of National Intelligence, the Director of the Central Intelligence Agency, and the Director of the Information Security Oversight Office, provide the National Security Advisor with a detailed concept of operations for the Center and a proposed implementing directive under section 5.1 of this order that reflects the coordinated views of the aforementioned agencies.

Part 4--Safeguarding

Sec. 4.1. General Restrictions on Access

(a) A person may have access to classified information provided that:

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

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

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

(b) Every person who has met the standards for access to classified information in paragraph (a) of this section shall receive contemporaneous training on the

proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

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

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

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

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

(1) prevent access by unauthorized persons;

(2) ensure the integrity of the information; and

(3) to the maximum extent practicable, use:

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

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

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

(h) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When

adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. "Confidential" information, including modified handling and transmission and allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

(i)(1) Classified information originating in one agency may be disseminated to another agency or U.S. entity by any agency to which it has been made available without the consent of the originating agency, as long as the criteria for access under section 4.1(a) of this order are met, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information in accordance with implementing directives issued pursuant to this order.

(2) Classified information originating in one agency may be disseminated by any other agency to which it has been made available to a foreign government in accordance with statute, this order, directives implementing this order, direction of the President, or with the consent of the originating agency. For the purposes of this section, "foreign government" includes any element of a foreign government, or an international organization of governments, or any element thereof.

(3) Documents created prior to the effective date of this order shall not be disseminated outside any other agency to which they have been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information that originated within that agency.

(4) For purposes of this section, the Department of Defense shall be considered one agency, except that any dissemination of information regarding intelligence sources, methods, or activities shall be consistent with directives issued pursuant to section 6.2(b) of this order.

(5) Prior consent of the originating agency is not required when referring records for declassification review that contain information originating in more than one agency.

Sec. 4.2. Distribution Controls

(a) The head of each agency shall establish procedures in accordance with applicable law and consistent with directives issued pursuant to this order to ensure that classified information is accessible to the maximum extent possible by individuals who meet the criteria set forth in section 4.1(a) of this order.

(b) In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the agency head or any designee may authorize the

disclosure of classified information (including information marked pursuant to section 4.1(i)(1) of this order) to an individual or individuals who are otherwise not eligible for access. Such actions shall be taken only in accordance with directives implementing this order and any procedure issued by agencies governing the classified information, which shall be designed to minimize the classified information that is disclosed under these circumstances and the number of individuals who receive it. Information disclosed under this provision or implementing directives and procedures shall not be deemed declassified as a result of such disclosure or subsequent use by a recipient. Such disclosures shall be reported promptly to the originator of the classified information. For purposes of this section, the Director of National Intelligence may issue an implementing directive governing the emergency disclosure of classified intelligence information.

(c) Each agency shall update, at least annually, the automatic, routine, or recurring distribution mechanism for classified information that it distributes. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Sec. 4.3. Special Access Programs

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

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

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

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

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

(3) Special access programs shall be subject to the oversight program established under section 5.4(d) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director of the Information Security Oversight Office and no more than one other employee of the Information Security Oversight Office or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

(5) Upon request, an agency head shall brief the National Security Advisor, or a designee, on any or all of the agency's special access programs.

(6) For the purposes of this section, the term "agency head" refers only to the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each.

(c) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

Sec. 4.4. Access by Historical Researchers and Certain Former Government Personnel

(a) The requirement in section 4.1(a)(3) of this order that access to classified information may be granted only to individuals who have a need to know the information may be waived for persons who:

(1) are engaged in historical research projects;

(2) previously have occupied senior policy-making positions to which they were appointed or designated by the President or the Vice President; or

(3) served as President or Vice President.

(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

(1) determines in writing that access is consistent with the interest of the national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and

(3) limits the access granted to former Presidential appointees or designees and Vice Presidential appointees or designees to items that the person originated, reviewed, signed, or received while serving as a Presidential or Vice Presidential appointee or designee.

Part 5—Implementation and Review

Sec. 5.1. Program Direction

(a) The Director of the Information Security Oversight Office, under the direction of the Archivist and in consultation with the National Security Advisor, shall issue such directives as are necessary to implement this order. These directives shall be binding on the agencies. Directives issued by the Director of the Information Security Oversight Office shall establish standards for:

(1) classification, declassification, and marking principles;

(2) safeguarding classified information, which shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information;

(3) agency security education and training programs;

(4) agency self-inspection programs; and

(5) classification and declassification guides.

(b) The Archivist shall delegate the implementation and monitoring functions of this program to the Director of the Information Security Oversight Office.

(c) The Director of National Intelligence, after consultation with the heads of affected agencies and the Director of the Information Security Oversight Office, may issue directives to implement this order with respect to the protection of intelligence sources, methods, and activities. Such directives shall be consistent with this order and directives issued under paragraph (a) of this section.

Sec. 5.2. Information Security Oversight Office

(a) There is established within the National Archives an Information Security Oversight Office. The Archivist shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Archivist, acting in consultation with the National Security Advisor, the Director of the Information Security Oversight Office shall:

(1) develop directives for the implementation of this order;

(2) oversee agency actions to ensure compliance with this order and its implementing directives;

(3) review and approve agency implementing regulations prior to their issuance to ensure their consistency with this order and directives issued under section 5.1(a) of this order;

(4) have the authority to conduct onsite reviews of each agency's program established under this order, and to require of each agency those reports and information and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the President through the National Security Advisor within 60 days of the request for access. Access shall be denied pending the response;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the National Security Advisor;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;

(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;

(8) report at least annually to the President on the implementation of this order; and

(9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

Sec. 5.3. Interagency Security Classification Appeals Panel

(a) Establishment and administration.

(1) There is established an Interagency Security Classification Appeals Panel. The Departments of State, Defense, and Justice, the National Archives, the Office of the Director of National Intelligence, and the National Security Advisor shall

each be represented by a senior-level representative who is a full-time or permanent part-time Federal officer or employee designated to serve as a member of the Panel by the respective agency head. The President shall designate a Chair from among the members of the Panel.

(2) Additionally, the Director of the Central Intelligence Agency may appoint a temporary representative who meets the criteria in paragraph (a)(1) of this section to participate as a voting member in all Panel deliberations and associated support activities concerning classified information originated by the Central Intelligence Agency.

(3) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (a)(1) of this section.

(4) The Director of the Information Security Oversight Office shall serve as the Executive Secretary of the Panel. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(5) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

(6) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(7) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

(b) Functions. The Panel shall:

(1) decide on appeals by persons who have filed classification challenges under section 1.8 of this order;

(2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.3 of this order;

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.5 of this order; and

(4) appropriately inform senior agency officials and the public of final Panel decisions on appeals under sections 1.8 and 3.5 of this order.

(c) Rules and procedures. The Panel shall issue bylaws, which shall be published in the Federal Register. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals.

The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which:

(1) the appellant has exhausted his or her administrative remedies within the responsible agency;

(2) there is no current action pending on the issue within the Federal courts; and

(3) the information has not been the subject of review by the Federal courts or the Panel within the past 2 years.

(d) Agency heads shall cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. The Panel shall report to the President through the National Security Advisor any instance in which it believes that an agency head is not cooperating fully with the Panel.

(e) The Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless changed by the President.

(f) An agency head may appeal a decision of the Panel to the President through the National Security Advisor. The information shall remain classified pending a decision on the appeal.

Sec. 5.4. General Responsibilities

Heads of agencies that originate or handle classified information shall:

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

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

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

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

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

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

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

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

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

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

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

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

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

(A) original classification authorities;

(B) security managers or security specialists; and

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

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

(9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains

to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function; and

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

Sec. 5.5. Sanctions

(a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives has occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

(2) classify or continue the classification of information in violation of this order or any implementing directive;

(3) create or continue a special access program contrary to the requirements of this order; or

(4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b) of this section occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2), or (3) of this section occurs.

Part 6—General Provisions

Sec. 6.1. Definitions

For purposes of this order:

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

(b) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105; any "Military department" as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

(c) "Authorized holder" of classified information means anyone who satisfies the conditions for access stated in section 4.1(a) of this order.

(d) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(e) "Automatic declassification" means the declassification of information based solely upon:

(1) the occurrence of a specific date or event as determined by the original classification authority; or

(2) the expiration of a maximum time frame for duration of classification established under this order.

(f) "Classification" means the act or process by which information is determined to be classified information.

(g) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

(h) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(i) "Classified national security information" or "classified information" means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(j) "Compilation" means an aggregation of preexisting unclassified items of information.

(k) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(l) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

(m) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(n) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(o) "Derivative classification" means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(p) "Document" means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

(q) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(r) "File series" means file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

(s) "Foreign government information" means:
(1) information provided to the United States Government by a foreign government or governments,

an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) information received and treated as "foreign government information" under the terms of a predecessor order.

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

(u) "Infraction" means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a "violation," as defined below.

(v) "Integral file block" means a distinct component of a file series, as defined in this section, that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time, such as a Presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group. For purposes of automatic declassification, integral file blocks shall contain only records dated within 10 years of the oldest record in the file block.

(w) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(x) "Intelligence" includes foreign intelligence and counterintelligence as defined by Executive Order 12333 of December 4, 1981, as amended, or by a successor order.

(y) "Intelligence activities" means all activities that elements of the Intelligence Community are authorized to conduct pursuant to law or Executive Order 12333, as amended, or a successor order.

(z) "Intelligence Community" means an element or agency of the U.S. Government identified in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended, or section 3.5(h) of Executive Order 12333, as amended.

(aa) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of this order.

(bb) "Multiple sources" means two or more source documents, classification guides, or a combination of both.

(cc) "National security" means the national defense or foreign relations of the United States.

(dd) "Need-to-know" means a determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(ee) "Network" means a system of two or more computers that can exchange data or information.

(ff) "Original classification" means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

(gg) "Original classification authority" means an individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(hh) "Records" means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

(ii) "Records having permanent historical value" means Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.

(jj) "Records management" means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

(kk) "Safeguarding" means measures and controls that are prescribed to protect classified information.

(ll) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(mm) "Senior agency official" means the official designated by the agency head under section 5.4(d) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

(nn) "Source document" means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(oo) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

(pp) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with title 44, United States Code.

(qq) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(rr) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(ss) "U.S. entity" includes:

(1) State, local, or tribal governments;

(2) State, local, and tribal law enforcement and firefighting entities;

(3) public health and medical entities;

(4) regional, state, local, and tribal emergency management entities, including State Adjutants General and other appropriate public safety entities; or

(5) private sector entities serving as part of the nation's Critical Infrastructure/Key Resources.

(tt) "Violation" means:

(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or

(3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

(uu) "Weapons of mass destruction" means any weapon of mass destruction as defined in 50 U.S.C. 1801(p).

Sec. 6.2. General Provisions

(a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Director of National Intelligence may, with respect to the Intelligence Community and after consultation with the heads of affected departments and agencies, issue such policy directives and guidelines as the Director of National Intelligence deems necessary to implement this order with respect to the classification and declassification of all intelligence and intelligence-related information, and for access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered. Procedures or other guidance issued by Intelligence Community element heads shall be in accordance with such policy directives or guidelines issued by the Director of National Intelligence. Any such policy directives or guidelines issued by the Director of National Intelligence shall be in accordance with directives issued by the Director of the Information Security Oversight Office under section 5.1(a) of this order.

(c) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(d) Nothing in this order limits the protection afforded any information by other provisions of law, including the Constitution, Freedom of Information Act exemptions, the Privacy Act of 1974, and the National Security Act of 1947, as amended. This order is not intended to and does not create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any

other person. The foregoing is in addition to the specific provisos set forth in sections 1.1(b), 3.1(c) and 5.3(e) of this order.

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

(f) This order shall be implemented subject to the availability of appropriations.

(g) Executive Order 12958 of April 17, 1995, and amendments thereto, including Executive Order 13292 of March 25, 2003, are hereby revoked as of the effective date of this order.

Sec. 6.3. Effective Date

This order is effective 180 days from the date of this order, except for sections 1.7, 3.3, and 3.7, which are effective immediately.

Sec. 6.4. Publication

The Archivist of the United States shall publish this Executive Order in the Federal Register.

BARACK OBAMA

THE WHITE HOUSE,
December 29, 2009.

Executive Order 12,958: Classified National Security Information (Superseded)

As Amended Through January 1, 2010

Exec. Order No. 12,958, *Classified National Security Information*, 60 Fed. Reg. 19826 (April 17, 1995), *available at* http://www.intelligencelaw.com/library/admin/html/eo_12958-4-17-1995.html.

Table of Contents

Preamble

"This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security remains a priority.

"NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Part 1 : Original Classification

1.1 Classification Standards

"(a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

"(1) an original classification authority is classifying the information;

"(2) the information is owned by, produced by or for, or is under the control of the United States Government;

"(3) the information falls within one or more of the categories of information listed in Section 1.4 of this order; and

"(4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

"(b) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

"(c) The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.

1.2 Classification Levels

"(a) Information may be classified at one of the following three levels:

"(1) 'Top Secret' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

"(2) 'Secret' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

"(3) 'Confidential' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

"(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

1.3 Classification Authority

"(a) The authority to classify information originally may be exercised only by:

"(1) the President and, in the performance of executive duties, the Vice President;

"(2) agency heads and officials designated by the President in the Federal Register; and

"(3) United States Government officials delegated this authority pursuant to paragraph (c) of this section.

"(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

"(c) Delegation of original classification authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

"(2) 'Top Secret' original classification authority may be delegated only by the President; in the performance of executive duties, the Vice President; or an agency head or official designated pursuant to paragraph (a)(2) of this section.

"(3) 'Secret' or 'Confidential' original classification authority may be delegated only by the President; in the performance of executive duties, the Vice President; or an agency head or official designated pursuant to paragraph (a)(2) of this section; or the senior agency official described in section 5.4(d) of this order, provided that official has been delegated 'Top Secret' original classification authority by the agency head.

"(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position title.

"(d) Original classification authorities must receive training in original classification as provided in this order and its implementing directives. Such training must include instruction on the proper safeguarding of classified information and of the criminal, civil, and administrative sanctions that may be brought against an individual who fails to protect classified information from unauthorized disclosure.

"(e) Exceptional cases. When an employee, government contractor, licensee, certificate holder, or grantee of an agency who does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

1.4 Classification Categories

Information shall not be considered for classification unless it concerns:

"(a) military plans, weapons systems, or operations;

"(b) foreign government information;

"(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;

"(d) foreign relations or foreign activities of the United States, including confidential sources;

"(e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;

"(f) United States Government programs for safeguarding nuclear materials or facilities;

"(g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or

"(h) weapons of mass destruction.

1.5 Duration of Classification

"(a) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. The date or event shall not exceed the time frame established in paragraph (b) of this section.

"(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it shall be marked for declassification for up to 25 years from the date of the original decision. All information classified under this section shall be subject to section 3.3 of this order if it is contained in records of permanent historical value under title 44, United States Code.

"(c) An original classification authority may extend the duration of classification, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this order are followed.

"(d) Information marked for an indefinite duration of classification under predecessor orders, for example, marked as 'Originating Agency's Determination Required,' or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with part 3 of this order.

1.6 Identification and Markings

"(a) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner:

"(1) one of the three classification levels defined in Section 1.2 of this order;

"(2) the identity, by name or personal identifier and position, of the original classification authority;

"(3) the agency and office of origin, if not otherwise evident;

"(4) declassification instructions, which shall indicate one of the following: (A) the date or event for declassification, as prescribed in Section 1.5(a) or Section 1.5(c);

"(B) the date that is 10 years from the date of original classification, as prescribed in Section 1.5(b); or

"(C) the date that is up to 25 years from the date of original classification, as prescribed in Section 1.5 (b); and

"(5) a concise reason for classification that, at a minimum, cites the applicable classification categories in Section 1.4 of this order.

"(b) Specific information described in paragraph (a) of this section may be excluded if it would reveal additional classified information.

"(c) With respect to each classified document, the agency originating the document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are

unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant waivers of this requirement. The Director shall revoke any waiver upon a finding of abuse.

"(d) Markings implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

"(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking provided that the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.

"(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

"(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

"(h) Prior to public release, all declassified records shall be appropriately marked to reflect their declassification.

1.7 Classification Prohibitions and Limitations

"(a) In no case shall information be classified in order to:

"(1) conceal violations of law, inefficiency, or administrative error;

"(2) prevent embarrassment to a person, organization, or agency;

"(3) restrain competition; or

"(4) prevent or delay the release of information that does not require protection in the interest of the national security.

"(b) Basic scientific research information not clearly related to the national security shall not be classified.

"(c) Information may be reclassified after declassification and release to the public under proper authority only in accordance with the following conditions:

"(1) the reclassification action is taken under the personal authority of the agency head or deputy agency head, who determines in writing that the reclassification of the information is necessary in the interest of the national security;

"(2) the information may be reasonably recovered; and

"(3) the reclassification action is reported promptly to the Director of the Information Security Oversight Office.

"(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.5 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.4 of this order.

"(e) Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that: (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information. As used in this order, 'compilation' means an aggregation of pre-existing unclassified items of information.

1.8 Classification Challenges

(a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b) of this section.

"(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall ensure that:

"(1) individuals are not subject to retribution for bringing such actions;

"(2) an opportunity is provided for review by an impartial official or panel; and

"(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel (Panel) established by section 5.3 of this order.

Part 2: Derivative Classification

2.1 Use of Derivative Classification

(a) Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

"(b) Persons who apply derivative classification markings shall:

"(1) observe and respect original classification decisions; and

"(2) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

"(A) the date or event for declassification that corresponds to the longest period of classification among the sources; and

"(B) a listing of these sources on or attached to the official file or record copy.

2.2 Classification Guides

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

"(b) Each guide shall be approved personally and in writing by an official who:

"(1) has program or supervisory responsibility over the information or is the senior agency official; and

"(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

"(c) Agencies shall establish procedures to ensure that classification guides are reviewed and updated as provided in directives issued under this order.

Part 3: Declassification and Downgrading

3.1 Authority for Declassification

(a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

"(b) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure. This provision does not:

"(1) amplify or modify the substantive criteria or procedures for classification; or

"(2) create any substantive or procedural rights subject to judicial review.

"(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the Assistant to the President for National Security Affairs. The information shall remain classified pending a prompt decision on the appeal.

"(d) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

3.2 Transferred Records

(a) In the case of classified records transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

"(b) In the case of classified records that are not officially transferred as described in paragraph (a) of this section, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such records shall be deemed to be the originating agency for purposes of this order. Such records may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the records.

"(c) Classified records accessioned into the National Archives and Records Administration (National Archives) as of the effective date of this order shall be declassified or downgraded by the Archivist of the United States (Archivist) in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

"(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that classified records be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to records being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or records for which the National Archives serves as the custodian of the records of an agency or organization that has gone out of existence.

"(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in section 3.3 of this order.

3.3 Automatic Declassification

(a) Subject to paragraphs (b)-(e) of this section, on December 31, 2006, all classified records that (1) are more than 25 years old and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of its original classification, except as provided in paragraphs (b)-(e) of this section.

"(b) An agency head may exempt from automatic declassification under paragraph (a) of this section specific information, the release of which could be expected to:

"(1) reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;

"(2) reveal information that would assist in the development or use of weapons of mass destruction;

"(3) reveal information that would impair U.S. cryptologic systems or activities;

"(4) reveal information that would impair the application of state of the art technology within a U.S. weapon system;

"(5) reveal actual U.S. military war plans that remain in effect;

"(6) reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

"(7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

"(8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or

"(9) violate a statute, treaty, or international agreement.

"(c) An agency head shall notify the President through the Assistant to the President for National Security Affairs of any specific file series of records for which a review or assessment has determined that the information within that file series almost invariably falls within one or more of the exemption categories listed in paragraph (b) of this section and which the agency proposes to exempt from automatic declassification. The notification shall include:

"(1) a description of the file series;

"(2) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and

"(3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b) of this section, a specific date or event for declassification of the information. The President may direct the agency head not to exempt the file series or to declassify the information within that series at an earlier date than recommended. File series exemptions previously approved by the President shall remain valid without any additional agency action.

"(d) At least 180 days before information is automatically declassified under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Panel, of any specific information beyond that included in a notification to the President under paragraph (c) of this section that the agency proposes to exempt from automatic declassification. The notification shall include:

"(1) a description of the information, either by reference to information in specific records or in the form of a declassification guide;

"(2) an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and

"(3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b) of this section, a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. The agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

"(e) The following provisions shall apply to the onset of automatic declassification:

"(1) Classified records within an integral file block, as defined in this order, that are otherwise subject to automatic declassification under this section shall not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block.

"(2) By notification to the Director of the Information Security Oversight Office, before the records are subject to automatic declassification, an agency head or senior agency official designated under section 5.4 of this order may delay automatic declassification for up to 5 additional years for classified information contained in microforms, motion pictures, audiotapes, videotapes, or comparable media that make a review for possible declassification exemptions more difficult or costly.

"(3) By notification to the Director of the Information Security Oversight Office, before the records are subject to automatic declassification, an agency head or senior agency official designated under section 5.4 of this order may delay automatic declassification for up to 3 years for classified records that have been referred or transferred to that agency by another agency less than 3 years before automatic declassification would otherwise be required.

"(4) By notification to the Director of the Information Security Oversight Office, an agency head or senior agency official designated under section 5.4 of this order may delay automatic declassification for up to 3 years from the date of discovery of classified records that were inadvertently not reviewed prior to the effective date of automatic declassification.

"(f) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

"(g) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

"(h) Records containing information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies shall be referred for review to those agencies and the information of concern shall be

subject to automatic declassification only by those agencies, consistent with the provisions of subparagraphs (e)(3) and (e)(4) of this section.

3.4 Systematic Declassification Review

(a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to records of permanent historical value exempted from automatic declassification under section 3.3 of this order. Agencies shall prioritize the systematic review of records based upon the degree of researcher interest and the likelihood of declassification upon review.

"(b) The Archivist shall conduct a systematic declassification review program for classified records: (1) accessioned into the National Archives as of the effective date of this order; (2) transferred to the Archivist pursuant to section 2203 of title 44, United States Code; and (3) for which the National Archives serves as the custodian for an agency or organization that has gone out of existence. This program shall apply to pertinent records no later than 25 years from the date of their creation. The Archivist shall establish priorities for the systematic review of these records based upon the degree of researcher interest and the likelihood of declassification upon review. These records shall be reviewed in accordance with the standards of this order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office shall ensure that agencies provide the Archivist with adequate and current declassification guides.

"(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

3.5 Mandatory Declassification Review

(a) Except as provided in paragraph (b) of this section, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

"(1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

"(2) the information is not exempted from search and review under sections 105C, 105D, or 701 of the National Security Act of 1947 (50 U.S.C. 403-5c, 403-5e, and 431); and

"(3) the information has not been reviewed for declassification within the past 2 years. If the agency has reviewed the information within the past 2 years, or the information is the subject of pending litigation, the agency shall inform the requester of this fact and of the requester's appeal rights.

"(b) Information originated by:

"(1) the incumbent President or, in the performance of executive duties, the incumbent Vice President;

"(2) the incumbent President's White House Staff or, in the performance of executive duties, the incumbent Vice President's Staff;

"(3) committees, commissions, or boards appointed by the incumbent President; or

"(4) other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a) of this section. However, the Archivist shall have the authority to review, downgrade, and declassify papers or records of former Presidents under the control of the Archivist pursuant to sections 2107, 2111, 2111 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Panel. The information shall remain classified pending a prompt decision on the appeal.

"(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

"(d) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Panel.

"(e) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information; the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods; and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

3.6 Processing Requests and Reviews

In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974 [5 U.S.C. §§ 552, 552a], or the mandatory review provisions of this order, or pursuant to the automatic declassification or systematic review provisions of this order:

"(a) An agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified under this order or its predecessors.

"(b) When an agency receives any request for documents in its custody that contain information that was originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order or its predecessors. In cases in which the originating agency determines in writing that a response under paragraph (a) of this section is required, the referring agency shall respond to the requester in accordance with that paragraph.

3.7 Declassification Database

(a) The Director of the Information Security Oversight Office, in conjunction with those agencies that originate classified information, shall coordinate the linkage and effective utilization of existing agency databases of records that have been declassified and publicly released.

"(b) Agency heads shall fully cooperate with the Director of the Information Security Oversight Office in these efforts.

Part 4: Safeguarding

4.1 General Restrictions on Access

(a) A person may have access to classified information provided that:

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

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

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

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

"(c) Classified information shall remain under the control of the originating agency or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.

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

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

"(f) Consistent with law, directives, and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that

collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

"(1) prevent access by unauthorized persons; and

"(2) ensure the integrity of the information.

"(g) Consistent with law, directives, and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

"(h) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States 'Confidential' information, including modified handling and transmission and allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved non-disclosure agreement.

"(i) Except as otherwise provided by statute, this order, directives implementing this order, or by direction of the President, classified information originating in one agency shall not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this section, the Department of Defense shall be considered one agency. Prior consent is not required when referring records for declassification review that contain information originating in several agencies.

4.2 Distribution Controls

(a) Each agency shall establish controls over the distribution of classified information to ensure that it is distributed only to organizations or individuals eligible for access and with a need-to-know the information.

"(b) In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the agency head or any designee may authorize the disclosure of classified information to an individual or individuals who are otherwise not eligible for access. Such actions shall be taken only in accordance with the directives implementing this order and any procedures issued by agencies governing the classified information, which shall be designed to minimize the classified information that is disclosed under these circumstances and the number of individuals who receive it. Information disclosed under this provision or implementing directives and procedures shall not be deemed declassified as a result of such disclosure or subsequent use by a recipient. Such disclosures shall be reported promptly to the originator of the classified information. For purposes of this section, the Director of Central Intelligence

may issue an implementing directive governing the emergency disclosure of classified intelligence information.

"(c) Each agency shall update, at least annually, the automatic, routine, or recurring distribution of classified information that they distribute. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

4.3 Special Access Programs

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

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

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

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

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

"(3) Special access programs shall be subject to the oversight program established under section 5.4(d) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office, or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

"(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

"(5) Upon request, an agency head shall brief the Assistant to the President for National Security Affairs, or a designee, on any or all of the agency's special access programs.

"(c) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

4.4 Access by Historical Researchers and Certain Former Government Personnel

(a) The requirement in section 4.1(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

"(1) are engaged in historical research projects;

"(2) previously have occupied policy-making positions to which they were appointed by the President under section 105(a)(2)(A) of title 3, United States Code, or the Vice President under 106(a)(1)(A) of title 3, United States Code; or

"(3) served as President or Vice President.

"(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

"(1) determines in writing that access is consistent with the interest of the national security;

"(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and

"(3) limits the access granted to former Presidential appointees and Vice Presidential appointees to items that the person originated, reviewed, signed, or received while serving as a Presidential appointee or a Vice Presidential appointee.

Part 5: Implementation and Review

5.1 Program Direction

(a) The Director of the Information Security Oversight Office, under the direction of the Archivist and in consultation with the Assistant to the President for National Security Affairs, shall issue such directives as are necessary to implement this order. These directives shall be binding upon the agencies. Directives issued by the Director of the Information Security Oversight Office shall establish standards for:

"(1) classification and marking principles;

"(2) safeguarding classified information, which shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information;

"(3) agency security education and training programs;

"(4) agency self-inspection programs; and

"(5) classification and declassification guides.

"(b) The Archivist shall delegate the implementation and monitoring functions of this program to the Director of the Information Security Oversight Office.

5.2 Information Security Oversight Office

(a) There is established within the National Archives an Information Security Oversight Office. The Archivist shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

"(b) Under the direction of the Archivist, acting in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

"(1) develop directives for the implementation of this order;

"(2) oversee agency actions to ensure compliance with this order and its implementing directives;

"(3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;

"(4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the President through the Assistant to the President for National Security Affairs within 60 days of the request for access. Access shall be denied pending the response;

"(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the Assistant to the President for National Security Affairs;

"(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;

"(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;

"(8) report at least annually to the President on the implementation of this order; and

"(9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

5.3 Interagency Security Classification Appeals Panel

(a) Establishment and administration.

(1) There is established an Interagency Security Classification Appeals Panel. The Departments of State, Defense, and Justice, the Central Intelligence Agency, the National Archives, and the Assistant to the President for National Security Affairs shall each be represented by a senior-level representative who is a full-time or permanent part-time Federal officer or employee designated to serve as a member of the Panel by the respective agency head. The President shall select the Chair of the Panel from among the Panel members.

"(2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (a)(1) of this section.

"(3) The Director of the Information Security Oversight Office shall serve as the Executive Secretary. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

"(4) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

"(5) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

"(6) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

"(b) Functions. The Panel shall:

"(1) decide on appeals by persons who have filed classification challenges under Section 1.8 of this order;

"(2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.3 of this order; and

"(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.5 of this order.

"(c) Rules and procedures. The Panel shall issue bylaws, which shall be published in the Federal Register. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which:

"(1) the appellant has exhausted his or her administrative remedies within the responsible agency;

"(2) there is no current action pending on the issue within the Federal courts; and

"(3) the information has not been the subject of review by the Federal courts or the Panel within the past 2 years.

"(d) Agency heads shall cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the Assistant to the President for National Security Affairs. The Panel shall report to the President through the Assistant to the President for National Security Affairs any instance in which it believes that an agency head is not cooperating fully with the Panel.

"(e) The Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless changed by the President.

"(f) Notwithstanding paragraphs (a) through (e) of this section, whenever the Panel reaches a conclusion that information owned or controlled by the Director of Central Intelligence (Director) should be declassified, and the Director notifies the Panel that he objects to its conclusion because he has determined that the information could reasonably be expected to cause damage to the national security and to reveal (1) the identity of a human intelligence source, or (2) information about the application of an intelligence source or method (including any information that concerns, or is provided as a result of, a relationship with a cooperating intelligence element of a foreign government), the information shall remain classified unless the Director's determination is appealed to the President, and the President reverses the determination.

5.4 General Responsibilities

Heads of agencies that originate or handle classified information shall:

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

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

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

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

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

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

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

"(4) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;

"(5) establishing procedures to prevent unnecessary access to classified information, including procedures that:

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

"(B) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs;

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

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

"(A) original classification authorities;

"(B) security managers or security specialists; and

"(C) all other personnel whose duties significantly involve the creation or handling of classified information;

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

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

5.5 Sanctions

(a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives has occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

"(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

"(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

"(2) classify or continue the classification of information in violation of this order or any implementing directive;

"(3) create or continue a special access program contrary to the requirements of this order; or

"(4) contravene any other provision of this order or its implementing directives.

"(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

"(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

"(e) The agency head or senior agency official shall:

"(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b) of this section occurs; and

"(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2), or (3) of this section occurs.

Part 6: General Provisions

6.1 Definitions

For purposes of this order:

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

"(b) 'Agency' means any 'Executive agency,' as defined in 5 U.S.C. 105; any 'Military department' as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

"(c) 'Automated information system' means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

"(d) 'Automatic declassification' means the declassification of information based solely upon:

"(1) the occurrence of a specific date or event as determined by the original classification authority; or

"(2) the expiration of a maximum time frame for duration of classification established under this order.

"(e) 'Classification' means the act or process by which information is determined to be classified information.

"(f) 'Classification guidance' means any instruction or source that prescribes the classification of specific information.

"(g) 'Classification guide' means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

"(h) 'Classified national security information' or 'classified information' means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

"(i) 'Confidential source' means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

"(j) 'Damage to the national security' means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

"(k) 'Declassification' means the authorized change in the status of information from classified information to unclassified information.

"(l) 'Declassification authority' means:

"(1) the official who authorized the original classification, if that official is still serving in the same position;

"(2) the originator's current successor in function;

"(3) a supervisory official of either; or

"(4) officials delegated declassification authority in writing by the agency head or the senior agency official.

"(m) 'Declassification guide' means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

"(n) 'Derivative classification' means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

"(o) 'Document' means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

"(p) 'Downgrading' means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

"(q) 'File series' means file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

"(r) 'Foreign government information' means:

"(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

"(2) information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

"(3) information received and treated as 'foreign government information' under the terms of a predecessor order.

"(s) 'Information' means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. 'Control' means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

"(t) 'Infraction' means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a 'violation,' as defined below.

"(u) 'Integral file block' means a distinct component of a file series, as defined in this section, that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time such as presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group.

"(v) 'Integrity' means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

"(w) 'Mandatory declassification review' means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of this order.

"(x) 'Multiple sources' means two or more source documents, classification guides, or a combination of both.

"(y) 'National security' means the national defense or foreign relations of the United States.

"(z) 'Need-to-know' means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific

classified information in order to perform or assist in a lawful and authorized governmental function.

"(aa) 'Network' means a system of two or more computers that can exchange data or information.

"(bb) 'Original classification' means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

"(cc) 'Original classification authority' means an individual authorized in writing, either by the President, the Vice President in the performance of executive duties, or by agency heads or other officials designated by the President, to classify information in the first instance.

"(dd) 'Records' means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

"(ee) 'Records having permanent historical value' means Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.

"(ff) 'Records management' means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

"(gg) 'Safeguarding' means measures and controls that are prescribed to protect classified information.

"(hh) 'Self-inspection' means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

"(ii) 'Senior agency official' means the official designated by the agency head under section 5.4(d) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

"(jj) 'Source document' means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

"(kk) 'Special access program' means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

"(ll) 'Systematic declassification review' means the review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with title 44, United States Code.

"(mm) 'Telecommunications' means the preparation, transmission, or communication of information by electronic means.

"(nn) 'Unauthorized disclosure' means a communication or physical transfer of classified information to an unauthorized recipient.

"(oo) 'Violation' means:

"(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

"(2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or

"(3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

"(pp) 'Weapons of mass destruction' means chemical, biological, radiological, and nuclear weapons.

6.2 General Provisions

(a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954 [42 U.S.C. §§ 2011 et seq. generally; for full classification, consult U.S.C. Tables volumes], as amended, or the National Security Act of 1947 [50 U.S.C. §§ 401 et seq. generally; for full classification, consult U.S.C. Tables volumes], as amended. 'Restricted Data' and 'Formerly Restricted Data' shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

"(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

"(c) Nothing in this order limits the protection afforded any information by other provisions of law, including the Constitution, Freedom of Information Act [5 U.S.C. § 552] exemptions, the Privacy Act of 1974 [5 U.S.C. § 552a], and the National Security Act of 1947 [50 U.S.C. §§ 401 et seq. generally; for full classification, consult U.S.C. Tables volumes], as amended. This order is not intended to and does not create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its departments, agencies, officers, employees, or agents. The foregoing is in addition to the specific provisos set forth in sections 3.1(b) and 5.3(e) of this order."

"(d) Executive Order 12356 of April 6, 1982 [former note to this section], was revoked as of October 14, 1995.

6.3 Effective Date

This order is effective immediately, except for Section 1.6, which shall become effective 180 days from the date of this order.

II. AGENCY RULES

Legislative and Non-Legislative Rules Relevant to U.S. Intelligence Law

Department of Defense Regulation 5240.1-R: Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons

December 1982

U.S. Dep't of Defense, Reg. No. 5240.1-R, Procedures Governing the Activities of DOD Intelligence Components that Affect U.S. Persons (Dec. 1982), *available at* http://www.intelligencelaw.com/library/admin/html/dodr_5240-1-R_1982.html.

Table of Contents

REFERENCES

- Executive Order 12333, "United States Intelligence Activities," December 4, 1981
- Public Law 95-511, "Foreign Intelligence Surveillance Act of 1978"
- DoD Directive 5200.29, "DoD Technical Surveillance Countermeasures (TSCM) Survey Program," February 12, 1975
- Chapters 105 and 119 of title 18, United States Code
- Public Law 73-416, "Communications Act of 1934," Section 605
- Sections 801-840 of title 10, United States Code, "Uniform Code of Military Justice"
- Agreement Between the Deputy Secretary of Defense and Attorney General, April 5, 1979
- Executive Order 12198, "Prescribing Amendments to the Manual for Courts-Martial, United States, 1969," March 12, 1980
- DoD Directive 5525.5, "DoD Cooperation with Civilian Law Enforcement Officials," March 22, 1982
- DoD Directive 5000.11, "Data Elements and Data Codes Standardization Program," December 7, 1964
- DoD Directive 5000.19, "Policies for the Management and Control of Information Requirements," March 12, 1976

DL1. DEFINITIONS

DL1.1.1. Administrative Purposes

Information is collected for "administrative purposes" when it is necessary for the administration of the component concerned, but is not collected directly in performance of the intelligence activities assigned such component. Examples include information relating to the past performance of potential contractors; information to enable such components to discharge their public affairs and legislative duties, including the maintenance of correspondence files; the maintenance of employee personnel and training records; and training materials or documents produced at training facilities.

DL1.1.2. Available Publicly

Information that has been published or broadcast for general public consumption, is available on request to a member of the general public, could lawfully be seen or heard by any casual observer, or is made available at a meeting open to the general public. In this context, the "general public" also means general availability to persons in a military community even though the military community is not open to the civilian general public.

DL1.1.3. Communications Security

Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such telecommunications.

DL1.1.4. Consent

The agreement by a person or organization to permit DoD intelligence components to take particular actions that affect the person or organization. Consent may be oral or written unless a specific form of consent is required by a particular procedure. Consent may be implied if adequate notice is provided that a particular action (such as entering a building) carries with it the presumption of consent to an accompanying action (such as search of briefcases). (Questions regarding what is adequate notice in particular circumstances should be referred to the legal office responsible for advising the DoD intelligence component concerned.)

DL1.1.5. 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, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

DL1.1.6. Counterintelligence Investigation

Includes inquiries and other activities undertaken to determine whether a particular United States person is acting for, or on behalf of, a foreign power for purposes of conducting espionage and other intelligence activities, sabotage, assassinations, international terrorist activities, and actions to neutralize such acts.

DL1.1.7. DoD Component

Includes the Office of the Secretary of Defense, each of the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies.

DL1.1.8. DoD Intelligence Components

Include the following organizations:

- DL1.1.8.1. The National Security Agency/Central Security Service.
- DL1.1.8.2. The Defense Intelligence Agency.
- DL1.1.8.3. The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.
- DL1.1.8.4. The Assistant Chief of Staff for Intelligence, Army General Staff.
- DL1.1.8.5. The Office of Naval Intelligence.
- DL1.1.8.6. The Assistant Chief of Staff, Intelligence, U. S. Air Force.
- DL1.1.8.7. The Army Intelligence and Security Command.
- DL1.1.8.8. The Naval Intelligence Command.
- DL1.1.8.9. The Naval Security Group Command.
- DL1.1.8.10. The Director of Intelligence, U.S. Marine Corps.
- DL1.1.8.11. The Air Force Intelligence Service.
- DL1.1.8.12. The Electronic Security Command, U.S. Air Force.
- DL1.1.8.13. The counterintelligence elements of the Naval Investigative Service.
- DL1.1.8.14. The counterintelligence elements of the Air Force Office of Special Investigations.
- DL1.1.8.15. The 650th Military Intelligence Group, SHAPE.
- DL1.1.8.16. Other organizations, staffs, and offices, when used for foreign intelligence or counterintelligence activities to which part 2 of E.O. 12333 (reference (a)), applies, provided that the heads of such organizations, staffs, and offices shall not be considered as heads of DoD intelligence components for purposes of this Regulation.

DL1.1.9. Electronic Surveillance

Acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio

direction finding equipment solely to determine the location of a transmitter. (Electronic surveillance within the United States is subject to the definitions in the Foreign Intelligence Surveillance Act of 1978 (reference (b)).)

DL1.1.10. Employee

A person employed by, assigned to, or acting for an agency within the intelligence community, including contractors and persons otherwise acting at the direction of such an agency.

DL1.1.11. Foreign Intelligence

Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities.

DL1.1.12. Foreign Power

Any foreign government (regardless of whether recognized by the United States), foreign-based political party (or faction thereof), foreign military force, foreign-based terrorist group, or any organization composed, in major part, of any such entity or entities.

DL1.1.13. Intelligence Activities

Refers to all activities that DoD intelligence components are authorized to undertake pursuant to Executive Order 12333 (reference (a)).

DL1.1.14. Intelligence Community and an Agency of Or Within the Intelligence Community

Refers to the following organizations:

- DL1.1.14.1. The Central Intelligence Agency (CIA).
- DL1.1.14.2. The National Security Agency (NSA).
- DL1.1.14.3. The Defense Intelligence Agency (DIA).
- DL1.1.14.4. The Offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs.
- DL1.1.14.5. The Bureau of Intelligence and Research of the Department of State.
- DL1.1.14.6. The intelligence elements of the Army, the Navy, the Air Force and the Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy.
- DL1.1.14.7. The staff elements of the Office of the Director of Central Intelligence.

DL1.1.15. International Narcotics Activities

Refers to activities outside the United States to produce, transfer or sell narcotics or other substances controlled in accordance with Sections 811 and 812 of title 21, United States Code.

DL1.1.16. International Terrorist Activities

Activities undertaken by or in support of terrorists or terrorist organizations that occur totally outside the United States, or that transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which the perpetrators operate or seek asylum.

DL1.1.17. Lawful Investigation

An investigation qualifies as a lawful investigation if the subject of the investigation is within DoD investigative jurisdiction; if it is conducted by a DoD Component that has authorization to conduct the particular type of investigation concerned (for example, counterintelligence, personnel security, physical security, communications security); and if the investigation is conducted in accordance with applicable law and policy, including E.O. 12333 and this Regulation.

DL1.1.18. Personnel Security

Measures designed to insure that persons employed, or being considered for employment, in sensitive positions of trust are suitable for such employment with respect to loyalty, character, emotional stability, and reliability and that such employment is clearly consistent with the interests of the national security. It includes measures designed to ensure that persons granted access to classified information remain suitable for such access and that access is consistent with the interests of national security.

DL1.1.19. Personnel Security Investigation:

- DL1.1.19.1. An inquiry into the activities of a person granted access to intelligence or other classified information; or a person who is being considered for access to intelligence or other classified information, including persons who are granted or may be granted access to facilities of DoD intelligence components; or a person to be assigned or retained in a position with sensitive duties.emsp [sic]; The investigation is designed to develop information pertaining to the suitability, eligibility, and trustworthiness of the individual with respect to loyalty, character, emotional stability and reliability.
- DL1.1.19.2. Inquiries and other activities directed against DoD employees or members of a Military Service to determine the facts of possible voluntary or involuntary compromise of classified information by them.
- DL1.1.19.3. The collection of information about or from military personnel in the course of tactical training exercises for security training purposes.

DL1.1.20. Physical Security

The physical measures taken to prevent unauthorized access to, and prevent the damage or loss of, equipment, facilities, materiel and documents; and measures undertaken to protect DoD personnel from physical threats to their safety.

DL1.1.21. Physical Security Investigation

All inquiries, inspections, or surveys of the effectiveness of controls and procedures designed to provide physical security; and all inquiries and other actions undertaken to obtain information pertaining to physical threats to DoD personnel or property.

DL1.1.22. Reasonable Belief

A reasonable belief arises when the facts and circumstances are such that a reasonable person would hold the belief. Reasonable belief must rest on facts and circumstances that can be articulated; "hunches" or intuitions are not sufficient. Reasonable belief can be based on experience, training, and knowledge in foreign intelligence or counterintelligence work applied to facts and circumstances at hand, so that a trained and experienced "reasonable person" might hold a reasonable belief sufficient to satisfy this criterion when someone unfamiliar with foreign intelligence or counterintelligence work might not.

DL1.1.23. Signals Intelligence

A category of intelligence including communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, either individually or in combination.

DL1.1.24. United States

When used to describe a place, the term shall include the territories under the sovereignty of the United States.

DL1.1.25. United States Person

DL1.1.25.1. The term "United States person" means:

- DL1.1.25.1.1. A United States citizen;
- DL1.1.25.1.2. An alien known by the DoD intelligence component concerned to be a permanent resident alien;
- DL1.1.25.1.3. An unincorporated association substantially composed of United States citizens or permanent resident aliens;
- DL1.1.25.1.4. A corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the United States, is not a United States person.

DL1.1.25.2. A person or organization outside the United States shall be presumed not to be a United States person unless specific information to the contrary is

obtained. An alien in the United States shall be presumed not to be a United States person unless specific information to the contrary is obtained.

DL1.1.25.3. A permanent resident alien is a foreign national lawfully admitted into the United States for permanent residence.

C1. CHAPTER 1: PROCEDURE 1. GENERAL PROVISIONS

C1.1. APPLICABILITY AND SCOPE

C1.1.1. These procedures apply only to "DoD intelligence components," as defined in the Definitions Section. Procedures 2 through 4 provide the sole authority by which such components may collect, retain and disseminate information concerning United States persons. Procedures 5 through 10 set forth applicable guidance with respect to the use of certain collection techniques to obtain information for foreign intelligence and counterintelligence purposes. Authority to employ such techniques shall be limited to that necessary to perform functions assigned the DoD intelligence component concerned. Procedures 11 through 15 govern other aspects of DoD intelligence activities, including the oversight of such activities.

C1.1.2. The functions of DoD intelligence components not specifically addressed herein shall be carried out in accordance with applicable policy and procedure.

C1.1.3. These procedures do not apply to law enforcement activities, including civil disturbance activities, that may be undertaken by DoD intelligence components. When an investigation or inquiry undertaken pursuant to these procedures establishes reasonable belief that a crime has been committed, the DoD intelligence component concerned shall refer the matter to the appropriate law enforcement agency in accordance with procedures 12 and 15 or, if the DoD intelligence component is otherwise authorized to conduct law enforcement activities, shall continue such investigation under appropriate law enforcement procedures.

C1.1.4. DoD intelligence components shall not request any person or entity to undertake any activity forbidden by Executive Order 12333 (reference (a)).

C1.2. PURPOSE

The purpose of these procedures is to enable DoD intelligence components to carry out effectively their authorized functions while ensuring their activities that affect U.S. persons are carried out in a manner that protects the constitutional rights and privacy of such persons.

C1.3. INTERPRETATION

C1.3.1. These procedures shall be interpreted in accordance with their stated purpose.

C1.3.2. All defined terms appear in the Definitions Section. Additional terms, not otherwise defined, are explained in the text of each procedure, as appropriate.

C1.3.3. All questions of interpretation shall be referred to the legal office responsible for advising the DoD intelligence component concerned. Questions that cannot be resolved in this manner shall be referred to the General Counsel of the Military Department concerned, or, as appropriate, the General Counsel of the Department of Defense for resolution.

C1.4. EXCEPTIONS TO POLICY

Requests for exception to the policies and procedures established herein shall be made in writing to the Deputy Under Secretary of Defense (Policy), who shall obtain the written approval of the Secretary of Defense and, if required, the Attorney General for any such exception.

C1.5. AMENDMENT

Requests for amendment of these procedures shall be made to the Deputy Under Secretary of Defense (Policy), who shall obtain the written approval of the Secretary of Defense, and, if required, the Attorney General, for any such amendment.

C2. CHAPTER 2: PROCEDURE 2. COLLECTION OF INFORMATION ABOUT UNITED STATES PERSONS

C2.1. APPLICABILITY AND SCOPE

This procedure specifies the kinds of information about United States persons that may be collected by DoD intelligence components and sets forth general criteria governing the means used to collect such information. Additional limitations are imposed in Procedures 5 through 10 on the use of specific collection techniques.

C2.2. EXPLANATION OF UNDEFINED TERMS

C2.2.1. When Information is Considered to be "Collected"

Information shall be considered as "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties. Thus, information volunteered to a DoD intelligence component by a cooperating source would be "collected" under this procedure when an employee of such component officially accepts, in some manner, such information for use within that component. Data acquired by electronic means is "collected" only when it has been processed into intelligible form.

C2.2.2. "Cooperating Sources"

Cooperating sources means persons or organizations that knowingly and voluntarily provide information to DoD intelligence components, or access to information, at the request of such components or on their own initiative. These include Government Agencies, law enforcement authorities, credit agencies, academic institutions, employers, and foreign governments.

C2.2.3. "Domestic Activities"

Domestic activities refers to activities that take place within the United States that do not involve a significant connection with a foreign power, organization, or person.

C2.2.4. "Overt"

Overt means refers to methods of collection whereby the source of the information being collected is advised, or is otherwise aware, that he is providing such information to the Department of Defense or a component thereof.

C2.3. TYPES OF INFORMATION THAT MAY BE COLLECTED ABOUT UNITED STATES PERSONS

Information that identifies a United States person may be collected by a DoD intelligence component only if it is necessary to the conduct of a function assigned the collecting component, and only if it falls within one of the following categories:

C2.3.1. Information Obtained With Consent

Information may be collected about a United States person who consents to such collection.

C2.3.2. Publicly Available Information

Information may be collected about a United States person if it is publicly available.

C2.3.3. Foreign Intelligence

Subject to the special limitation contained in section C2.5., below, information may be collected about a United States person if the information constitutes foreign intelligence, provided the intentional collection of foreign intelligence about United States persons shall be limited to persons who are:

- C2.3.3.1. Individuals reasonably believed to be officers or employees, or otherwise acting for or on behalf, of a foreign power;
- C2.3.3.2. An organization reasonably believed to be owned or controlled, directly or indirectly, by a foreign power;
- C2.3.3.3. Persons or organizations reasonably believed to be engaged or about to engage, in international terrorist or international narcotics activities;
- C2.3.3.4. Persons who are reasonably believed to be prisoners of war; missing in action; or are the targets, the hostages, or victims of international terrorist organizations; or
- C2.3.3.5. Corporations or other commercial organizations believed to have some relationship with foreign powers, organizations, or persons.

C2.3.4. Counterintelligence

Information may be collected about a United States person if the information constitutes counterintelligence, provided the intentional collection of counterintelligence about United States persons must be limited to:

- C2.3.4.1. Persons who are reasonably believed to be engaged in, or about to engage in, intelligence activities on behalf of a foreign power, or international terrorist activities.
- C2.3.4.2. Persons in contact with persons described in subparagraph C2.3.4.1., above, for the purpose of identifying such person and assessing their relationship with persons described in subparagraph C2.3.4.1., above.

C2.3.5. Potential Sources of Assistance to Intelligence Activities

Information may be collected about United States persons reasonably believed to be potential sources of intelligence, or potential sources of assistance to intelligence activities, for the purpose of assessing their suitability or credibility. This category does not include investigations undertaken for personnel security purposes.

C2.3.6. Protection of Intelligence Sources and Methods

Information may be collected about a United States person who has access to, had access to, or is otherwise in possession of, information that reveals foreign intelligence and counterintelligence sources or methods, when collection is reasonably believed necessary to protect against the unauthorized disclosure of such information; provided that within the United States, intentional collection of such information shall be limited to persons who are:

- C2.3.6.1. Present and former DoD employees;
- C2.3.6.2. Present or former employees of a present or former DoD contractor; and
- C2.3.6.3. Applicants for employment at the Department of Defense or at a contractor of the Department of Defense.

C2.3.7. Physical Security

Information may be collected about a United States person who is reasonably believed to threaten the physical security of DoD employees, installations, operations, or official visitors. Information may also be collected in the course of a lawful physical security investigation.

C2.3.8. Personnel Security

Information may be collected about a United States person that arises out of a lawful personnel security investigation.

C2.3.9. Communications Security

Information may be collected about a United States person that arises out of a lawful communications security investigation.

C2.3.10. Narcotics

Information may be collected about a United States person who is reasonably believed to be engaged in international narcotics activities.

C2.3.11. Threats to Safety

Information may be collected about a United States person when the information is needed to protect the safety of any person or organization, including those who are targets, victims, or hostages of international terrorist organizations.

C2.3.12. Overhead Reconnaissance

Information may be collected from overhead reconnaissance not directed at specific United States persons.

C2.3.13. Administrative Purposes

Information may be collected about a United States person that is necessary for administrative purposes.

C2.4. GENERAL CRITERIA GOVERNING THE MEANS USED TO COLLECT INFORMATION ABOUT UNITED STATES PERSONS

C2.4.1. Means of Collection

DoD intelligence components are authorized to collect information about United States persons by any lawful means, provided that all such collection activities shall be carried out in accordance with E.O. 12333 (reference (a)), and this Regulation, as appropriate.

C2.4.2. Least Intrusive Means

The collection of information about United States persons shall be accomplished by the least intrusive means. In general, this means the following:

- C2.4.2.1. To the extent feasible, such information shall be collected from publicly available information or with the consent of the person concerned;
- C2.4.2.2. If collection from these sources is not feasible or sufficient, such information may be collected from cooperating sources;
- C2.4.2.3. If collection from cooperating sources is not feasible or sufficient, such information may be collected, as appropriate, using other lawful investigative techniques that do not require a judicial warrant or the approval of the Attorney General; then
- C2.4.2.4. If collection through use of these techniques is not feasible or sufficient, approval for use of investigative techniques that do require a judicial warrant or the approval of the Attorney General may be sought.

C2.5. SPECIAL LIMITATION ON THE COLLECTION OF FOREIGN INTELLIGENCE WITHIN THE UNITED STATES

Within the United States, foreign intelligence concerning United States persons may be collected only by overt means unless all the following conditions are met:

- C2.5.1. The foreign intelligence sought is significant and collection is not undertaken for the purpose of acquiring information concerning the domestic activities of any United States person;
- C2.5.2. Such foreign intelligence cannot be reasonably obtained by overt means;
- C2.5.3. The collection of such foreign intelligence has been coordinated with the Federal Bureau of Investigation (FBI); and
- C2.5.4. The use of other than overt means has been approved in writing by the head of the DoD intelligence component concerned, or his single designee, as being consistent with these procedures. A copy of any approval made pursuant to this section shall be provided the Deputy Under Secretary of Defense (Policy).

C3. CHAPTER 3: PROCEDURE 3. RETENTION OF INFORMATION ABOUT UNITED STATES PERSONS

C3.1. APPLICABILITY

This procedure governs the kinds of information about United States persons that may knowingly be retained by a DoD intelligence component without the consent of the person whom the information concerns. It does not apply when the information in question is retained solely for administrative purposes or is required by law to be maintained.

C3.2. EXPLANATION OF UNDEFINED TERMS

The term "retention," as used in this procedure, refers only to the maintenance of information about United States persons that can be retrieved by reference to the person's name or other identifying data.

C3.3. CRITERIA FOR RETENTION

C3.3.1. Retention of Information Collected Under Procedure 2

Information about United States persons may be retained if it was collected pursuant to Procedure 2.

C3.3.2. Retention of Information Acquired Incidentally

Information about United States persons collected incidentally to authorized collection may be retained if:

- C3.3.2.1. Such information could have been collected intentionally under Procedure 2;
- C3.3.2.2. Such information is necessary to understand or assess foreign intelligence or counterintelligence;
- C3.3.2.3. The information is foreign intelligence or counterintelligence collected from electronic surveillance conducted in compliance with this Regulation; or
- C3.3.2.4. Such information is incidental to authorized collection and may indicate involvement in activities that may violate Federal, State, local, or foreign law.

C3.3.3. Retention of Information Relating to Functions of Other DoD Components or non-DoD Agencies

Information about United States persons that pertains solely to the functions of other DoD Components or Agencies outside the Department of Defense shall be retained only as necessary to transmit or deliver such information to the appropriate recipients.

C3.3.4. Temporary Retention

Information about United States persons may be retained temporarily, for a period not to exceed 90 days, solely for the purpose of determining whether that information may be permanently retained under these procedures.

C3.3.5. Retention of Other Information

Information about United States persons other than that covered by paragraphs C3.3.1. through C3.3.4., above, shall be retained only for purposes of reporting such collection for oversight purposes and for any subsequent proceedings that may be necessary.

C3.4. ACCESS AND RETENTION

C3.4.1. Controls On Access to Retained Information

Access within a DoD intelligence component to information about United States persons retained pursuant to this procedure shall be limited to those with a need to know.

C3.4.2. Duration of Retention

Disposition of information about United States Persons retained in the files of DoD intelligence components will comply with the disposition schedules approved by the Archivist of the United States for the files or records in which the information is retained.

C3.4.3. Information Acquired Prior to Effective Date

Information acquired prior to the effective date of this procedure may be retained by DoD intelligence components without being screened for compliance with this procedure or Executive Order 12333 (reference (a)), so long as retention was in compliance with applicable law and previous Executive orders.

C4. CHAPTER 4: PROCEDURE 4. DISSEMINATION OF INFORMATION ABOUT UNITED STATES PERSONS

C4.1. APPLICABILITY AND SCOPE

This procedure governs the kinds of information about United States persons that may be disseminated, without their consent, outside the DoD intelligence component that collected and retained the information. It does not apply to information collected solely for administrative purposes; or disseminated pursuant to law; or pursuant to a court order that otherwise imposes controls upon such dissemination.

C4.2. CRITERIA FOR DISSEMINATION

Except as provided in section C4.3., below, information about United States persons that identifies those persons may be disseminated without the consent of those persons only under the following conditions:

- C4.2.1. The information was collected or retained or both under Procedures 2 and 3;
- C4.2.2. The recipient is reasonably believed to have a need to receive such information for the performance of a lawful governmental function, and is one of the following:
    - C4.2.2.1. An employee of the Department of Defense, or an employee of a contractor of the Department of Defense, and has a need for such information in the course of his or her official duties;
    - C4.2.2.2. A law enforcement entity of Federal, State, or local government, and the information may indicate involvement in activities that may violate laws that the recipient is responsible to enforce;
    - C4.2.2.3. An Agency within the intelligence community; provided that within the intelligence community, information other than information derived from signals intelligence, may be disseminated to each appropriate Agency for the purpose of allowing the recipient Agency to determine whether the information is relevant to its responsibilities without such a determination being required of the disseminating DoD intelligence component;
    - C4.2.2.4. An Agency of the Federal Government authorized to receive such information in the performance of a lawful governmental function; or
    - C4.2.2.5. A foreign government, and dissemination is undertaken pursuant to an agreement or other understanding with such government.

C4.3. OTHER DISSEMINATION

Any dissemination that does not conform to the conditions set forth in section C4.2., above, must be approved by the legal office responsible for advising the

DoD Component concerned after consultation with the Department of Justice and General Counsel of the Department of Defense. Such approval shall be based on determination that the proposed dissemination complies with applicable laws, Executive orders, and regulations.

C5. CHAPTER 5: PROCEDURE 5. ELECTRONIC SURVEILLANCE

C5.1. PART 1: ELECTRONIC SURVEILLANCE IN THE UNITED STATES FOR INTELLIGENCE PURPOSES

C5.1.1. Applicability

This part of Procedure 5 implements the Foreign Intelligence Surveillance Act of 1979 (reference (b)), and applies to electronic surveillance, as defined in that Act, conducted by DoD intelligence components within the United States to collect "foreign intelligence information," as defined in that Act.

C5.1.2. General Rules

- C5.1.2.1. Electronic Surveillance Pursuant to the Foreign Intelligence Surveillance Act

A DoD intelligence component may conduct electronic surveillance within the United States for foreign intelligence and counterintelligence purposes only pursuant to an order issued by a judge of the court appointed pursuant to the Foreign Intelligence Surveillance Act of 1978 (reference (b)), or pursuant to a certification of the Attorney General issued under the authority of Section 102(a) of the Act.

- C5.1.2.2. Authority to Request Electronic Surveillance

Authority to approve the submission of applications or requests for electronic surveillance under the Foreign Intelligence Surveillance Act of 1978 (reference (b)) shall be limited to the Secretary of Defense, the Deputy Secretary of Defense, the Secretary or Under Secretary of a Military Department, and the Director of the National Security Agency. Applications for court orders will be made through the Attorney General after prior clearance by the General Counsel, DoD. Requests for Attorney General certification shall be made only after prior clearance by the General Counsel, DoD.

- C5.1.2.3. Electronic Surveillance In Emergency Situations

C5.1.2.3.1. A DoD intelligence component may conduct electronic surveillance within the United States in emergency situations under an approval from the Attorney General in accordance with Section 105(e) of reference (b).

C5.1.2.3.2. The head of a DoD intelligence component may request that the DoD General Counsel seek such authority directly from the Attorney General in an emergency, if it is not feasible to submit such request through an official designated in subparagraph C5.1.2.2., above, provided the appropriate official concerned shall be advised of such requests as soon as possible thereafter.

C5.2. PART 2: ELECTRONIC SURVEILLANCE OUTSIDE THE UNITED STATES FOR INTELLIGENCE PURPOSES

C5.2.1. Applicability

This part of Procedure 5 applies to electronic surveillance, as defined in the Definitions Section, for foreign intelligence and counterintelligence purposes directed against United States persons who are outside the United States, and who, under the circumstances, have a reasonable expectation of privacy. It is intended to be applied in conjunction with the regulation of electronic surveillance "within the United States" under Part 1 and the regulation of "signals intelligence activities" under Part 3 so that the intentional interception for foreign intelligence and counterintelligence purposes of all wire or radio communications of persons within the United States and against United States persons abroad where such persons enjoy a reasonable expectation of privacy is covered by one of the three parts. In addition, this part governs the use of electronic, mechanical, or other surveillance devices for foreign intelligence and counterintelligence purposes against a United States person broad in circumstances where such person has a reasonable expectation of privacy. This part does not apply to the electronic surveillance of communications of other than United States persons abroad or the interception of the communications of United States persons abroad that do not constitute electronic surveillance.

C5.2.2. Explanation of Undefined Terms

- C5.2.2.1. “Directed against a United States Person”

Electronic surveillance is "directed against a United States person" when the surveillance is intentionally targeted against or designed to intercept the communications of that person. Electronic surveillance directed against persons who are not United States persons that results in the incidental acquisition of the communications of a United States person does not thereby become electronic surveillance directed against a United States person.

- C5.2.2.2. “Outside the United States”

Electronic surveillance is "outside the United States" if the person against whom the electronic surveillance is directed is physically outside the United States, regardless of the location at which surveillance is conducted. For example, the interception of communications that originate and terminate outside the United States can be conducted from within the United States and still fall under this part rather than Part 1.

C5.2.3. Procedures

Except as provided in paragraph C5.2.5., below, DoD intelligence components may conduct electronic surveillance against a United States person who is outside the United States for foreign intelligence and counterintelligence purposes only if the surveillance is approved by the Attorney General. Requests for approval will be forwarded to the Attorney General by an official designated in subparagraph C5.2.5.1., below. Each request shall include:

- C5.2.3.1. An identification or description of the target.

- C5.2.3.2. A statement of the facts supporting a finding that:
    - C5.2.3.2.1. There is probable cause to believe the target of the electronic surveillance is one of the following:
        - C5.2.3.2.1.1. A person who, for or on behalf of a foreign power is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or international terrorist activities, or activities in preparation for international terrorist activities; or who conspires with, or knowingly aids and abets a person engaging in such activities;
        - C5.2.3.2.1.2. A person who is an officer or employee of a foreign power;
        - C5.2.3.2.1.3. A person unlawfully acting for, or pursuant to the direction of, a foreign power. The mere fact that a person's activities may benefit or further the aims of a foreign power is not enough to bring that person under this paragraph, absent evidence that the person is taking direction from, or acting in knowing concert with, the foreign power;
        - C5.2.3.2.1.4. A corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or
        - C5.2.3.2.1.5. A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access.

        C5.2.3.2.2. The electronic surveillance is necessary to obtain significant foreign intelligence or counterintelligence.
    - C5.2.3.2.3. The significant foreign intelligence or counterintelligence expected to be obtained from the electronic surveillance could not reasonably be obtained by other less intrusive collection techniques.
- C5.2.3.3. A description of the significant foreign intelligence or counterintelligence expected to be obtained from the electronic surveillance.
- C5.2.3.4. A description of the means by which the electronic surveillance will be effected.
- C5.2.3.5. If physical trespass is required to effect the surveillance, a statement of facts supporting a finding that the means involve the least amount of intrusion that will accomplish the objective.
- C5.2.3.6. A statement of period of time, not to exceed 90 days, for which the electronic surveillance is required.
- C5.2.3.7. A description of the expected dissemination of the product of the surveillance, including a description of the procedures that will govern the retention and dissemination of communications of or concerning United

States persons other than those targeted, acquired incidental to such surveillance.

C5.2.4. Electronic Surveillance in Emergency Situations

Notwithstanding paragraph C5.2.3., above, a DoD intelligence component may conduct surveillance directed at a United States person who is outside the United States in emergency situations under the following limitations:

- C5.2.4.1. Officials designated in paragraph C5.2.5., below, may authorize electronic surveillance directed at a United States person outside the United States in emergency situations, when securing the prior approval of the Attorney General is not practical because:
    - C5.2.4.1.1. The time required would cause failure or delay in obtaining significant foreign intelligence or counterintelligence and such failure or delay would result in substantial harm to the national security;
    - C5.2.4.1.2. A person's life or physical safety is reasonably believed to be in immediate danger; or C5.2.4.1.3. The physical security of a defense installation or Government property is reasonably believed to be in immediate danger.
- C5.2.4.2. Except for actions taken under subparagraph C5.2.4.1.2., above, any official authorizing such emergency surveillance shall find that one of the criteria contained in subparagraph C5.2.3.2.1., above, is met. Such officials shall notify the DoD General Counsel promptly of any such surveillance, the reason for authorizing such surveillance on an emergency basis, and the expected results.
- C5.2.4.3. The Attorney General shall be notified by the General Counsel, DoD, as soon as possible of the surveillance, the circumstances surrounding its authorization, and the results thereof, and such other information as may be required to authorize continuation of such surveillance.
- C5.2.4.4. Electronic surveillance authorized pursuant to this section may not continue longer than the time required for a decision by the Attorney General and in no event longer than 72 hours.

C5.2.5. Officials Authorized to Request and Approve Electronic Surveillance Outside the United States

- C5.2.5.1. The following officials may request approval of electronic surveillance outside the United States under paragraph C5.2.3., above, and approve emergency surveillance under paragraph C5.2.4., above:
    - C5.2.5.1.1. The Secretary and Deputy Secretary of Defense.
    - C5.2.5.1.2. The Secretaries and Under Secretaries of the Military Departments.
    - C5.2.5.1.3. The Director and Deputy Director of the National Security Agency/Chief, Central Security Service.

- C5.2.5.2. Authorization for emergency electronic surveillance under paragraph C5.2.4., may also be granted by:
    - C5.2.5.2.1. Any general or flag officer at the overseas location in question, having responsibility for either the subject of the surveillance, or responsibility for the protection of the persons, installations, or property that is endangered, or
    - C5.2.5.2.2. The Deputy Director for Operations, National Security Agency.

C5.3. PART 3: SIGNALS INTELLIGENCE ACTIVITIES
C5.3.1. Applicability and Scope

- C5.3.1.1. This procedure governs the conduct by the United States Signals Intelligence System of signals intelligence activities that involve the collection, retention, and dissemination of foreign communications and military tactical communications. Such activities may incidentally involve the collection of information concerning United States persons without their consent, or may involve communications originated or intended for receipt in the United States, without the consent of a party thereto.
- C5.3.1.2. This part of Procedure 5 shall be supplemented by a classified Annex promulgated by the Director, National Security Agency/Chief, Central Security Service, which shall also be approved by the Attorney General. That regulation shall provide that signals intelligence activities that constitute electronic surveillance, as defined in Parts 1, and 2 of this procedure, will be authorized in accordance with those parts. Any information collected incidentally about United States persons shall be subjected to minimization procedures approved by the Attorney General.

C5.3.2. Explanation of Undefined Terms

- C5.3.2.1. “Communications concerning a United States person”
    - Communications concerning a United States person are those in which the United States person is identified in the communication. A United States person is identified when the person's name, unique title, address or other personal identifier is revealed in the communication in the context of activities conducted by that person or activities conducted by others and related to that person. A reference to a product by brand name or manufacturer's name or the use of a name in a descriptive sense, as, for example, "Monroe Doctrine," is not an identification of a United States person.
- C5.3.2.2. “Interception”
    - Interception means the acquisition by the United States Signals Intelligence system through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligible form, but not including the display of signals on visual display devices intended to permit the examination of the technical

characteristics of the signals without reference to the information content carried by the signals.

- C5.3.2.3. "Military tactical communication"
  - Military tactical communications means United States and allied military exercise communications within the United States and abroad necessary for the production of simulated foreign intelligence and counterintelligence or to permit an analysis of communications security.
- C5.3.2.4. SIGINT Guidelines for Determining whether a person is a "United States Person."
  - For purposes of signals intelligence activities only, the following guidelines will apply in determining whether a person is a United States person:
    - C5.3.2.4.1. Person Known to be Currently in the United States
      - A person known to be currently in the United States will be treated as a United States person unless the nature of the person's communications or other available information concerning the person gives rise to a reasonable belief that such person is not a United States citizen or permanent resident alien.
    - C5.3.2.4.2. Person Known to be Currently Outside the United States
      - A person known to be currently outside the United States, or whose location is not known, will not be treated as a United States person unless the nature of the person's communications or other available information concerning the person give rise to a reasonable belief that such person is a United States citizen or permanent resident alien.
    - C5.3.2.4.3. Circumstances in which a Person Known to be an Alien Admitted for Permanent Residence may be assumed to have lost status as a United States Person
      - A person known to be an alien admitted for permanent residence may be assumed to have lost status as a United States person if the person leaves the United States and it is known that the person is not in compliance with the administrative formalities provided by law that enable such persons to reenter the United States without regard to the provisions of law that would otherwise restrict an alien's entry into the United States. The failure to follow the statutory procedures provides a reasonable basis to conclude that such alien has abandoned any intention of maintaining status as a permanent resident alien.

        - C5.3.2.4.4. Unincorporated Association whose Headquarters are located outside the United States
            - An unincorporated association whose headquarters are located outside the United States may be presumed not to be a United States person unless the collecting agency has information indicating that a substantial number of members are citizens of the United States or aliens lawfully admitted for permanent residence.
- C5.3.2.5. "United States Signals Intelligence System"
    - United States Signals Intelligence System means the unified organization for signals intelligence activities under the direction of the Director, National Security Agency/Chief, Central Security Service, comprised of the National Security Agency, the Central Security Service, the components of the Military Services authorized to conduct signals intelligence and such other entities (other than the Federal Bureau of Investigation) as are authorized by the National Security Council or the Secretary of Defense to conduct signals intelligence. FBI activities are governed by procedures promulgated by the Attorney General.

C5.3.3. Procedures

- C5.3.3.1. Foreign Communications
    - The United States Signals Intelligence System may collect, process, retain, and disseminate foreign communications that are also communications of or concerning United States persons, but only in accordance with the classified annex to this procedure.
- C5.3.3.2. Military Tactical Communications
    - The United States Signals Intelligence System may collect, process, retain, and disseminate military tactical communications that are also communications of or concerning United States persons but only in accordance with the classified annex to this procedure.
- C5.3.3.2.1. Collection
    - Collection efforts will be conducted in the same manner as in the case of signals intelligence for foreign intelligence purposes and must be designed in such a manner as to avoid to the extent feasible the intercept of communications not related to military exercises.
- C5.3.3.2.2. Retention and Processing
    - Military tactical communications may be retained and processed without deletion of references to United States persons who are participants in, or are otherwise mentioned in exercise-related communications, provided that the communications of United States persons not participating in the exercise that are inadvertently intercepted during the exercise shall be destroyed as soon as feasible.

- C5.3.3.2.3. Dissemination
  - Dissemination of military tactical communications and exercise reports or information files derived from such communications shall be limited to those authorities and persons participating in or conducting reviews and critiques of such exercise.

C5.4. PART 4: TECHNICAL SURVEILLANCE COUNTERMEASURES

C5.4.1. Applicability and Scope

This part of Procedure 5 applies to the use of electronic equipment to determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance. It implements Section 105(f)(2) of the Foreign Intelligence Surveillance Act (reference (b)).

C5.4.2. Explanation of Undefined Terms

The term technical surveillance countermeasures refers to activities authorized pursuant to DoD Directive 5200.29 (reference (c)), and, as used in this procedure, refers to the use of electronic surveillance equipment, or electronic or mechanical devices, solely for determining the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, or for determining the susceptibility of electronic equipment to unlawful electronic surveillance.

C5.4.3. Procedures

A DoD intelligence component may use technical surveillance countermeasures that involve the incidental acquisition of the nonpublic communications of United States persons without their consent, provided:

- C5.4.3.1. The use of such countermeasures has been authorized or consented to by the official in charge of the facility, organization, or installation where the countermeasures are to be undertaken;
- C5.4.3.2. The use of such countermeasures is limited in that necessary to determine the existence and capability of such equipment; and
- C5.4.3.3. Access to the content of communications acquired during the use of countermeasures is limited to persons involved directly in conducting such measures, and any content acquired is destroyed as soon as practical or upon completion of the particular use. However, if the content is acquired within the United States, only information that is necessary to protect against unauthorized electronic surveillance, or to enforce Chapter 119 of title 18, United States Code (reference (d)) and Section 605 of the Communication Act of 1934 (reference (e)), may be retained and disseminated only for these purposes. If acquired outside the United States, information that indicates a violation of Federal law, including the Uniform Code of Military Justice (reference (f)), or a clear and imminent threat to life or property, may also be disseminated to appropriate law enforcement authorities. A record of the types of communications and

information subject to acquisition by the illegal electronic surveillance equipment may be retained.

C5.5. PART 5: DEVELOPING, TESTING, AND CALIBRATION OF ELECTRONIC EQUIPMENT

C5.5.1. Applicability

This part of Procedure 5 applies to developing, testing, or calibrating electronic equipment that can intercept or process communications and noncommunications signals. It also includes research and development that needs electronic communications as a signal source.

C5.5.2. Procedures

- C5.5.2.1. Signals Authorized for Use
  - C5.5.2.1.1. The following may be used without restriction:
    - C5.5.2.1.1.1. Laboratory-generated signals.
    - C5.5.2.1.1.2. Communications signals with the consent of the communicator.
    - C5.5.2.1.1.3. Communications in the commercial or public service broadcast bands.
    - C5.5.2.1.1.4. Communications transmitted between terminals located outside of the United States not used by any known United States person.
    - C5.5.2.1.1.5. Noncommunications signals (including telemetry, and radar).
  - C5.5.2.1.2. Communications subject to lawful electronic surveillance under the provisions of Parts 1, 2, or 3, of this procedure may be used subject to the minimization procedures applicable to such surveillance.
  - C5.5.2.1.3. Any of the following may be used subject to the restrictions of subparagraph C5.5.2.2., below.
    - C5.5.2.1.3.1. Communications over official Government communications circuits with consent from an appropriate official of the controlling agency.
    - C5.5.2.1.3.2. Communications in the citizens and amateur-radio bands.
  - C5.5.2.1.4. Other signals may be used only when it is determined that it is not practical to use the signals described above and it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance. The restrictions of subparagraph C5.5.2.2., below, will apply in such cases. The Attorney General must approve use of signals pursuant to this subsection for the purpose of development, testing, or calibration when the period of use exceeds 90 days. When Attorney General approval is required, the DoD intelligence component shall submit a test proposal to the General Counsel, DoD, or the NSA General Counsel for transmission to the Attorney General for approval. The test

proposal shall state the requirement for a period beyond 90 days, the nature of the activity, the organization that will conduct the activity, and the proposed disposition of any signals or communications acquired during the activity.

- C5.5.2.2. Restrictions
  - For signals described in subparagraphs C5.5.2.1.3. and C5.5.2.1.4., above, the following restrictions apply:
    - C5.5.2.2.1. The surveillance shall be limited in scope and duration to that necessary for the purposes referred to in paragraph C5.5.1., above.
    - C5.5.2.2.2. No particular United States person shall be targeted intentionally without consent.
    - C5.5.2.2.3. The content of any communication shall:
      - C5.5.2.2.3.1. Be retained only when actually needed for the purposes referred to in paragraph C5.5.1., above;
      - C5.5.2.2.3.2. Be disseminated only to persons conducting the activity; and
      - C5.5.2.2.3.3. Be destroyed immediately upon completion of the activity.
    - C5.5.2.2.4. The technical parameters of a communication (such as frequency, modulation, bearing, signal strength, and time of activity) may be retained and used for the purposes outlined in paragraph C5.5.1., above, or for collection avoidance purposes. Such parameters may be disseminated to other DoD intelligence components and other entities authorized to conduct electronic surveillance or related development, testing, and calibration of electronic equipment provided such dissemination and use are limited to the purposes outlined in paragraph C5.5.1., or collection avoidance purposes. No content of any communication may be retained or used other than as provided in subparagraph C5.5.2.2.3., above.

C5.6. PART 6: TRAINING OF PERSONNEL IN THE OPERATION AND USE OF ELECTRONIC COMMUNICATIONS AND SURVEILLANCE EQUIPMENT

C5.6.1. Applicability

This part of Procedure 5 applies to the training of personnel by DoD intelligence components in the operation and use of electronic communications and surveillance equipment. It does not apply to the interception of communications with the consent of one of the parties to the communication or to the training of intelligence personnel by non-intelligence components.

C5.6.2. Procedures

- C5.6.2.1. Training Guidance
  - The training of personnel by DoD intelligence components in the operation and use of electronic communications and surveillance equipment shall include guidance concerning the requirements and restrictions of the Foreign Intelligence Surveillance Act of 1978 (reference (b)), and E.O. 12333 (reference (a)), with respect to the unauthorized acquisition and use of the content of communications of United States persons.
- C5.6.2.2. Training Limitations
  - C5.6.2.2.1. Except as permitted by paragraph C5.6.2.2.2. and C5.6.2.2.3., below, the use of electronic communications and surveillance equipment for training purposes is permitted, subject to the following limitations:
    - C5.6.2.2.1.1. To the maximum extent practical, use of such equipment for training purposes shall be directed against communications that are subject to lawful electronic surveillance for foreign intelligence and counterintelligence purposes under Parts 1, 2, and 3 of this procedure.
    - C5.6.2.2.1.2. The contents of private communications of nonconsenting United States persons may not be acquired aurally unless the person is an authorized target of electronic surveillance.
    - C5.6.2.2.1.3. The electronic surveillance will be limited in extent and duration to that necessary to train personnel in the use of the equipment.
  - C5.6.2.2.2. Public broadcasts, distress signals, or official U.S. Government communications may be monitored, provided that when Government Agency communications are monitored, the consent of an appropriate official is obtained.
  - C5.6.2.2.3. Minimal acquisition of information is permitted as required for calibration purposes.
- C5.6.2.3. Retention and Dissemination
  - Information collected during training that involves communications described in subparagraph C5.6.2.2.1.1., above, shall be retained and disseminated in accordance with minimization procedures applicable to that electronic surveillance. Information collected during training that does not involve communications described in subparagraph C5.6.2.2.1.1., above, or that is acquired inadvertently, shall be destroyed as soon as practical or upon completion of the training and may not be disseminated for any purpose. This limitation does not apply to distress signals.

C5.7. PART 7: CONDUCT OF VULNERABILITY AND HEARABILITY SURVEYS

C5.7.1. Applicability and Scope

This part of Procedure 5 applies to the conduct of vulnerability surveys and hearability surveys by DoD intelligence components.

C5.7.2. Explanation of Undefined Terms

- C5.7.2.1. "Vulnerability Survey"
    - The term vulnerability survey refers to the acquisition of radio frequency propagation and its subsequent analysis to determine empirically the vulnerability of the transmission media to interception by foreign intelligence services.
- C5.7.2.2. "Hearability Survey"
    - The term hearability survey refers to monitoring radio communications to determine whether a particular radio signal can be received at one or more locations and, if reception is possible, to determine the hearability of reception over time.

C5.7.3. Procedures

- C5.7.3.1. Conduct of Vulnerability Surveys
    - Nonconsensual surveys may be conducted to determine the potential vulnerability to intelligence services of a foreign power of transmission facilities of communications common carriers, other private commercial entities, and entities of the federal government, subject of the following limitations:
        - C5.7.3.1.1. No vulnerability survey may be conducted without the prior written approval of the Director, National Security Agency, or his designee.
        - C5.7.3.1.2. No transmission may be acquired aurally.
        - C5.7.3.1.3. No content of any transmission may be acquired by any means.
        - C5.7.3.1.4. No transmissions may be recorded.
        - C5.7.3.1.5. No report or log may identify any United States person or entity except to the extent of identifying transmission facilities that are vulnerable to surveillance by foreign powers. If the identities of the users of such facilities are not identical with the identities of the owners of the facilities, the identity of such users may be obtained but not from the content of the transmissions themselves, and may be included in such report or log. Reports may be disseminated. Logs may be disseminated only if required to verify results contained in reports.
- C5.7.3.2. Conduct of Hearability Surveys

- The Director, National Security Agency, may conduct, or may authorize the conduct by other Agencies, of hearability surveys of telecommunications that are transmitted in the United States.
    - C5.7.3.2.1. Collection. When practicable, consent will be secured from the owner or user of the facility against which the hearability survey is to be conducted prior to the commencement of the survey.
    - C5.7.3.2.2. Processing and Storage. Information collected during a hearability survey must processed and stored as follows:
        - C5.7.3.2.2.1. The content of communications may not be recorded or included in any report.
        - C5.7.3.2.2.2. No microwave transmission may be demultiplexed or demodulated for any purpose.
        - C5.7.3.2.2.3. No report or log may identify any person or entity except to the extent of identifying the transmission facility that can be intercepted from the intercept site. If the identities of the users of such facilities are not identical with the identities of the owners of the facilities, and their identities are relevant to the purpose for which the hearability survey has been conducted, the identity of such users may be obtained provided such identities may not be obtained from the contents of the transmissions themselves.
    - C5.7.3.2.3. Dissemination. Reports may be disseminated only within the U.S. Government. Logs may not be disseminated unless required to verify results contained in reports.

C6. CHAPTER 6: PROCEDURE 6. CONCEALED MONITORING

C6.1. APPLICABILITY AND SCOPE

C6.1.1. Where no warrant would be required

This procedure applies to concealed monitoring only for foreign intelligence and counterintelligence purposes conducted by a DoD intelligence component within the United States or directed against a United States person who is outside the United States where the subject of such monitoring does not have a reasonable expectation of privacy, as explained in section 6.2., below, and no warrant would be required if undertaken for law enforcement purposes.

C6.1.2. Situations where a warrant would be required shall be treated as "Electronic surveillance"

Concealed monitoring in the United States for foreign intelligence and counterintelligence purposes where the subject of such monitoring has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes shall be treated as "electronic surveillance within the United States" under Part 1 of Procedure 5, and processed pursuant to that procedure.

C6.1.3. Concealed monitoring of U.S. Person Abroad

Concealed monitoring for foreign intelligence and counterintelligence purposes of a United States person abroad where the subject of such monitoring has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes shall be treated as "electronic surveillance outside the United States" under Part 2 of Procedure 5, and processed pursuant to that procedure.

C6.1.4. Concealed monitoring involving signals intelligence

Concealed monitoring for foreign intelligence and counterintelligence purposes when the monitoring is a signals intelligence activity shall be conducted pursuant to Part 3 of Procedure 5.

C6.2. EXPLANATION OF UNDEFINED TERMS

C6.2.1. "Concealed Monitoring"

Concealed monitoring means targeting by electronic, optical, or mechanical devices a particular person or a group of persons without their consent in a surreptitious and continuous manner. Monitoring is surreptitious when it is targeted in a manner designed to keep the subject of the monitoring unaware of it. Monitoring is continuous if it is conducted without interruption for a substantial period of time.

C6.2.2. Monitoring "within the United States"

Monitoring is within the United States if the monitoring device, or the target of the monitoring, is located within the United States.

C6.2.3. Concealed Monitoring where the subject has a reasonable expectation of privacy

Whether concealed monitoring is to occur where the subject has a reasonable expectation of privacy is a determination that depends upon the circumstances of a particular case, and shall be made only after consultation with the legal office responsible for advising the DoD intelligence component concerned. Reasonable expectation of privacy is the extent to which a reasonable person in the particular circumstances involved is entitled to believe his or her actions are not subject to monitoring by electronic, optical, or mechanical devices. For example, there are ordinarily reasonable expectations of privacy in work spaces if a person's actions and papers are not subject to ready observation by others under normal working conditions. Conversely, a person walking out of his or her residence into a public street ordinarily would not have a reasonable expectation that he or she is not being observed or even photographed; however, such a person ordinarily would have an expectation of privacy within his or her residence.

C6.3. PROCEDURES

C6.3.1. Limitations On Use of Concealed Monitoring

Use of concealed monitoring under circumstances when the subject of such monitoring has no reasonable expectation of privacy is subject to the following limitations:

- C6.3.1.1. Inside the United States
  - Within the United States, a DoD intelligence component may conduct concealed monitoring only on an installation or facility owned or leased by the Department of Defense or otherwise in the course of an investigation conducted pursuant to the Agreement Between the Secretary of Defense and the Attorney General (reference (g)).
- C6.3.1.2. Outside the United States
  - Outside the United States, such monitoring may be conducted on installations and facilities owned or leased by the Department of Defense. Monitoring outside such facilities shall be conducted after coordination with appropriate host country officials, if such coordination is required by the governing Status of Forces Agreement, and with the Central Intelligence Agency.

C6.3.2. Required Determination

Concealed monitoring conducted under paragraph C6.3.1., requires approval by an official designated in paragraph C6.3.3., below, based on a determination that such monitoring is necessary to the conduct of assigned foreign intelligence or counterintelligence functions, and does not constitute electronic surveillance under Parts 1 or 2 of Procedure 5.

C6.3.3. Officials Authorized to Approve Concealed Monitoring

Officials authorized to approve concealed monitoring under this procedure include the Deputy Under Secretary of Defense (Policy); the Director, Defense Intelligence Agency; the Director, National Security Agency; the Assistant Chief of Staff for Intelligence, Department of Army; the Director, Naval Intelligence; the Director of Intelligence, U.S. Marine Corps; the Assistant Chief of Staff, Intelligence, U.S. Air Force; the Commanding General, Army Intelligence and Security Command; the Director, Naval Investigative Service; and the Commanding Officer, Air Force Office of Special Investigations.

C7. CHAPTER 7: PROCEDURE 7. PHYSICAL SEARCHES

C7.1. APPLICABILITY

This procedure applies to nonconsensual physical searches of any person or property within the United States and to physical searches of the person or property of a United States person outside the United States by DoD intelligence components for foreign intelligence or counterintelligence purposes. DoD intelligence components may provide assistance to the Federal Bureau of Investigation and other law enforcement authorities in accordance with Procedure 12.

C7.2. EXPLANATION OF UNDEFINED TERMS

Physical search means any intrusion upon a person or a person's property or possessions to obtain items of property or information. The term does not include examination of areas that are in plain view and visible to the unaided eye if no physical trespass is undertaken, and does not include examinations of abandoned property left in a public place. The term also does not include any intrusion authorized as necessary to accomplish lawful electronic surveillance conducted pursuant to Parts 1 and 2 of Procedure 5.

C7.3. PROCEDURES

C7.3.1. Nonconsensual Physical Searches Within the United States

- C7.3.1.1. Searches of Active Duty Military Personnel for Counterintelligence Purposes
  - The counterintelligence elements of the Military Departments are authorized to conduct nonconsensual physical searches in the United States for counterintelligence purposes of the person or property of active duty military personnel, when authorized by a military commander empowered to approve physical searches for law enforcement purposes pursuant to rule 315(d) of the Manual for Courts Martial, Executive Order 12198 (reference (h)), based upon a finding of probable cause to believe such persons are acting as agents of foreign powers. For purposes of this section, the term "agent of a foreign power" refers to an individual who meets the criteria set forth in subparagraph C7.3.1.2., below.
- C7.3.1.2. Other Nonconsensual Physical Searches
  - Except as permitted by section C7.1., above, DoD intelligence components may not conduct nonconsensual physical searches of persons and property within the United States for foreign intelligence or counterintelligence purposes. DoD intelligence components may, however, request the FBI to conduct such searches. All such requests, shall be in writing; shall contain the information required in subparagraphs C7.3.2.2.1., through

C7.3.2.2.2.6., below; and be approved by an official designated in subparagraph C7.3.2.2.2.3., below. A copy of each such request shall be furnished the General Counsel, DoD.

C7.3.2. Nonconsensual Physical Searches Outside the United States

- C7.3.2.1. Searches of Active Duty Military Personnel for Counterintelligence Purposes.
  - The counterintelligence elements of the Military Departments may conduct nonconsensual physical searches of the person or property of active duty military personnel outside the United States for counterintelligence purposes when authorized by a military commander empowered to approve physical searches for law enforcement purposes pursuant to rule 315(d) of the Manual for Courts Martial, Executive Order 12198 (reference (h)), based upon a finding of probable cause to believe such persons are acting as agents of foreign powers. For purposes of this section, the term "agent of a foreign power" refers to an individual who meets the criteria set forth in subparagraph C7.3.2.2.2., below.
- C7.3.2.2. Other Nonconsensual Physical Searches
  - DoD intelligence components may conduct other nonconsensual physical searches for foreign intelligence and counterintelligence purposes of the person or property of United States persons outside the United States only pursuant to the approval of the Attorney General. Requests for such approval will be forwarded by a senior official designated in subparagraph C7.3.2.3., below, to the Attorney General and shall include:
    - C7.3.2.2.1. An identification of the person or description of the property to be searched.
    - C7.3.2.2.2. A statement of facts supporting a finding that there is probable cause to believe the subject of the search is:
      - C7.3.2.2.2.1. A person who, for or on behalf of a foreign power, is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or international terrorist activities, activities in preparation for international terrorist activities, or who conspires with, or knowingly aids and abets a person engaging in such activities;
      - C7.3.2.2.2.2. A person who is an officer or employee of a foreign power;
      - C7.3.2.2.2.3. A person unlawfully acting for, or pursuant to the direction of, a foreign power. The mere fact that a person's activities may benefit or further the aims of a foreign power does not justify a nonconsensual physical search without evidence that

the person is taking direction from, or acting in knowing concert with, the foreign power;

- C7.3.2.2.2.4. A corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or
- C7.3.2.2.2.5. A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access.

- C7.3.2.2.3. A statement of facts supporting a finding that the search is necessary to obtain significant foreign intelligence or counterintelligence.
- C7.3.2.2.4. A statement of facts supporting a finding that the significant foreign intelligence or counterintelligence expected to be obtained could not be obtained by less intrusive means.
- C7.3.2.2.5. A description of the significant foreign intelligence or counterintelligence expected to be obtained from the search.
- C7.3.2.2.6. A description of the extent of the search and a statement of facts supporting a finding that the search will involve the least amount of physical intrusion that will accomplish the objective sought.
- C7.3.2.2.7. A description of the expected dissemination of the product of the search, including a description of the procedures that will govern the retention and dissemination of information about United States persons acquired incidental to the search.

- C7.3.2.3. Officials that may request approval of nonconsensual physical searches under subparagraph C7.3.2.2.

- Requests for approval of nonconsensual physical searches under subparagraph C7.3.2.2., must be made by:
  - C7.3.2.3.1. The Secretary or the Deputy Secretary of Defense;
  - C7.3.2.3.2. The Secretary or the Under Secretary of a Military Department;
  - C7.3.2.3.3. The Director, National Security Agency; or
  - C7.3.2.3.4. The Director, Defense Intelligence Agency.

C8. CHAPTER 8: PROCEDURE 8. SEARCHES AND EXAMINATION OF MAIL

C8.1. APPLICABILITY

This procedure applies to the opening of mail in United States postal channels, and the use of mail covers with respect to such mail, for foreign intelligence and counterintelligence purposes. It also applies to the opening of mail to or from United States persons where such activity is conducted outside the United States and such mail is not in United States postal channels.

C8.2. EXPLANATION OF UNDEFINED TERMS

C8.2.1. "Mail within United States Postal Channels"

Mail Within United States Postal Channels includes:

- C8.2.1.1. Mail while in transit within, among, and between the United States, its territories and possessions (including mail of foreign origin that is passed by a foreign postal administration, to the United States Postal Service for forwarding to a foreign postal administration under a postal treaty or convention, and mail temporarily in the hands of the United States Customs Service or the Department of Agriculture), Army-Air Force (APO) and Navy (FPO) post offices, and mail for delivery to the United Nations, NY; and
- C8.2.1.2. International mail en route to an addressee in the United States or its possessions after passage to United States Postal Service from a foreign postal administration or en route to an addressee abroad before passage to a foreign postal administration. As a rule, mail shall be considered in such postal channels until the moment it is delivered manually in the United States to the specific addressee named on the envelope, or his authorized agent.

C8.2.2. "To examine mail"

To examine mail means to employ a mail cover with respect to such mail.

C8.2.3. "Mail cover"

Mail cover means the process by which a record is made of any data appearing on the outside cover of any class of mail matter as permitted by law, other than that necessary for the delivery of mail or administration of the Postal Service.

C8.3. PROCEDURES

C8.3.1. Searches of Mail Within United States Postal Channels

- C8.3.1.1. Applicable postal regulations do not permit DoD intelligence components to detain or open first-class mail within United States postal channels for foreign intelligence and counterintelligence purposes, or to request such action by the U.S. Postal Service.

- C8.3.1.2. DoD intelligence components may request appropriate U.S. postal authorities to inspect, or authorize the inspection, of the contents of second-, third-, or fourth-class mail in United States postal channels, for such purposes, in accordance with applicable postal regulations. Such components may also request appropriate U.S. postal authorities to detain, or permit the detention of, mail that may become subject to search under this section, in accordance with applicable postal regulations.

C8.3.2. Searches of Mail Outside United States Postal Channels

- C8.3.2.1. DoD intelligence components are authorized to open mail to or from a United States person that is found outside United States postal channels only pursuant to the approval of the Attorney General. Requests for such approval shall be treated as a request for a nonconsensual physical search under subparagraph C7.3.2.2., of Procedure 7.
- C8.3.2.2. Heads of DoD intelligence components may authorize the opening of mail outside U.S. postal channels when both the sender and intended recipient are other than United States persons if such searches are otherwise lawful and consistent with any Status of Forces Agreement that may be in effect.

C8.3.3. Mail Covers

- C8.3.3.1. DoD intelligence components may request U.S. postal authorities to examine mail in U.S. postal channels, for counterintelligence purposes, in accordance with applicable postal regulations.
- C8.3.3.2. DoD intelligence components may also request mail covers with respect to mail to or from a United States person that is outside U.S. postal channels, in accordance with appropriate law and procedure of the host government, and any Status of Forces Agreement that may be effect.

C9. CHAPTER 9: PROCEDURE 9. PHYSICAL SURVEILLANCE

C9.1. APPLICABILITY

This procedure applies only to the physical surveillance of United States persons by DoD intelligence components for foreign intelligence and counterintelligence purposes. This procedure does not apply to physical surveillance conducted as part of a training exercise when the subjects are participants in the exercise.

C9.2. EXPLANATION OF UNDEFINED TERMS

The term physical surveillance means a systematic and deliberate observation of a person by any means on a continuing basis, or the acquisition of a nonpublic communication by a person not a party thereto or visibly present thereat through any means not involving electronic surveillance.

C9.3. PROCEDURES

C9.3.1. Criteria for Physical Surveillance In the United States

Within the United States, DoD Intelligence components may conduct nonconsensual physical surveillances for foreign intelligence and counterintelligence purposes against United States persons who are present or former employees of the intelligence component concerned; present or former contractors of such components or their present or former employees; applicants for such employment or contracting; or military persons employed by a non-intelligence element of a Military Service. Any physical surveillance within the United States that occurs outside a DoD installation shall be coordinated with the FBI and other law enforcement agencies, as may be appropriate.

C9.3.2. Criteria for Physical Surveillance Outside the United States

Outside the United States, DoD Intelligence components may conduct nonconsensual physical surveillance of United States persons in one of the categories identified in paragraph C9.3.1., above. In addition, such components may conduct physical surveillance of other United States persons in the course of a lawful foreign intelligence or counterintelligence investigation, provided:

- C9.3.2.1. Such surveillance is consistent with the laws and policy of the host government and does not violate any Status of Forces Agreement that may be in effect;
- C9.3.2.2. That physical surveillance of a United States person abroad to collect foreign intelligence may be authorized only to obtain significant information that cannot be obtained by other means.

C9.3.3. Required Approvals for Physical Surveillance

- C9.3.3.1. Persons Within DoD Investigative Jurisdiction. Physical surveillances within the United States or that involve United States persons within DoD investigative jurisdiction overseas may be approved

by the head of the DoD intelligence component concerned or by designated senior officials of such components in accordance with this procedure.

- C9.3.3.2. Persons Outside DoD Investigative Jurisdiction. Outside the United States, physical surveillances of United States persons who are not within the investigative jurisdiction of the DoD intelligence component concerned will be forwarded through appropriate channels to the Deputy Under Secretary of Defense (Policy) for approval. Such requests shall indicate coordination with the Central Intelligence Agency.

C10. CHAPTER 10: PROCEDURE 10. UNDISCLOSED PARTICIPATION IN ORGANIZATIONS

C10.1. APPLICABILITY

This procedure applies to participation by employees of DoD intelligence components in any organization within the United States, or any organization outside the United States that constitutes a United States person, when such participation is on behalf of any entity of the intelligence community. These procedures do not apply to participation in organizations for solely personal purposes.

C10.2. EXPLANATION OF UNDEFINED TERMS

C10.2.1. "Domestic Activities"

Domestic activities refers to activities that take place within the United States that do not involve a significant connection with a foreign power, organization or person.

C10.2.2. "Organization"

The term organization includes corporations and other commercial organizations, academic institutions, clubs, professional societies, associations, and any other group whose existence is formalized in some manner or otherwise functions on a continuing basis.

C10.2.3. "Organization within the United States"

An organization within the United States means all organizations physically located within the geographical boundaries of the United States whether or not they constitute a United States persons. Thus, a branch, subsidiary, or office of an organization within the United States, which is physically located outside the United States, is not considered as an organization within the United States.

C10.2.4. "Participation"

Participation refers to any action undertaken within the structure or framework of the organization involved. Such actions include serving as a representative or agent of the organization; acquiring membership; attending meetings not open to the public, including social functions for the organization as a whole; carrying out the work or functions of the organization; and contributing funds to the organization other than in payment for goods or services. Actions taken outside the organizational framework, however, do not constitute participation. Thus, attendance at meetings or social gatherings that involve organization members, but are not functions or activities of the organization itself does not constitute participation.

C10.2.5. "Participation on behalf of an agency within the intelligence community"

Participation is on behalf of an agency within the intelligence community when an employee is tasked or requested to take action within an organization for the benefit of such agency. Such employee may already be a member of the organization or may be asked to join. Actions undertaken for the benefit of an intelligence agency include collecting information, identifying potential sources or contacts, or establishing and maintaining cover. If a cooperating source furnishes information to an intelligence agency that he or she obtained by participation within an organization, but was not given prior direction or tasking by the intelligence agency to collect such information, then such participation was not on behalf of such agency.

C10.2.6. "Participation solely for personal purposes"

Participation is solely for personal purposes, if undertaken at the initiative and expense of the employee for the employee's benefit.

C10.3. PROCEDURES FOR UNDISCLOSED PARTICIPATION

Except as permitted herein, employees of DoD intelligence components may participate on behalf of such components in organizations within the United States, or in organizations outside the United States that constitute United States persons, only if their affiliation with the intelligence component concerned is disclosed to an appropriate official of the organization in accordance with section C10.4., below. Participation without such disclosure is permitted only if it is consistent with the limitations set forth in paragraph C10.3.1., below, and has been approved in accordance with paragraph C10.3.2., below.

C10.3.1. Limitations On Undisclosed Participation

- C10.3.1.1. Lawful Purpose. No undisclosed participation shall be permitted under this procedure unless it is essential to achieving a lawful foreign intelligence or counterintelligence purpose within the assigned mission of the collecting DoD intelligence component.
- C10.3.1.2. Limitations On Use of Undisclosed Participation for Foreign Intelligence Purposes Within the United States. Undisclosed participation may not be authorized within the United States for the purpose of collecting foreign intelligence from or about a United States person, nor to collect information necessary to assess United States persons as potential sources of assistance to foreign intelligence activities. This does not preclude the collection of information about such persons, volunteered by cooperating sources participating in organizations to which such persons belong, however, if otherwise permitted by Procedure 2.
- C10.3.1.3. Duration of Participation. Authorization to participate under subparagraphs C10.3.2.1., and C10.3.2.2., shall be limited to the period covered by such participation, which shall be no longer than 12 months.

Participation that lasts longer than 12 months shall be reapproved by the appropriate official on an annual basis in accordance with this procedure.

- C10.3.1.4. Participation for the Purpose of Influencing the Activities of the Organization or Its Members. No participation under this procedure shall be authorized for the purpose of influencing the activities of the organization in question, or its members, unless such participation is undertaken on behalf of the FBI in the course of a lawful investigation, or the organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power. Any DoD intelligence component that desires to undertake participation for such purpose shall forward its request to the Deputy Under Secretary of Defense (Policy) setting forth the relevant facts justifying such participation and explaining the nature of its contemplated activity. Such participation may be approved by the DUSD(P) with the concurrence of the General Counsel, DoD.

C10.3.2. Required Approvals

- C10.3.2.1. Undisclosed Participation That May Be Approved Within the DoD Intelligence Component. Undisclosed participation on behalf of a DoD intelligence component may be authorized with such component under the following circumstances:
    - C10.3.2.1.1. Participation in meetings open to the public. For purposes of this section, a seminar or conference sponsored by a professional organization that is open to persons of a particular profession, whether or not they are members of the organization itself or have received a special invitation, shall be considered a meeting open to the public.
    - C10.3.2.1.2. Participation in organizations that permit other persons acknowledged to the organization to be employees of the U.S. Government to participate.
    - C10.3.2.1.3. Participation in educational or professional organizations for the purpose of enhancing the professional skills, knowledge, or capabilities of employees.
    - C10.3.2.1.4. Participation in seminars, forums, conferences, exhibitions, trade fairs, workshops, symposiums, and similar types of meetings, sponsored by organizations in which the employee is a member, has been invited to participate, or when the sponsoring organization does not require disclosure of the participants' employment affiliations, for the purpose of collecting significant foreign intelligence that is generally made available to participants at such meetings, and does not involve the domestic activities of the organization or its members.
- C10.3.2.2. Participation That May Be Approved By Senior Intelligence Officials. Undisclosed participation may be authorized by the Deputy Under Secretary of Defense (Policy); the Director, Defense Intelligence

Agency; the Assistant Chief of Staff for Intelligence, Department of Army; the Commanding General, U.S. Army Intelligence and Security Command; the Director of Naval Intelligence; the Director of Intelligence, U.S. Marine Corps; the Assistant Chief of Staff, Intelligence, United States Air Force; the Director, Naval Investigative Service; the Commanding Officer, Air Force Office of Special Investigations; or their single designees, for the following purposes:

- C10.3.2.2.1. To collect significant foreign intelligence outside the United States, or from or about other than United States persons within the United States, provided no information involving the domestic activities of the organization or its members may be collected.
- C10.3.2.2.2. For counterintelligence purposes, at the written request of the Federal Bureau of Investigation.
- C10.3.2.2.3. To collect significant counterintelligence about other than United States persons, or about United States persons who are within the investigative jurisdiction of the Department of Defense, provided any such participation that occurs within the United States shall be coordinated with the Federal Bureau of Investigation.
- C10.3.2.2.4. To collect information necessary to identify and assess other than United States persons as potential sources of assistance for foreign intelligence and counterintelligence activities.
- C10.3.2.2.5. To collect information necessary to identify United States persons as potential sources of assistance to foreign intelligence and counterintelligence activities.
- C10.3.2.2.6. To develop or maintain cover necessary for the security of foreign intelligence or counterintelligence activities.
- C10.3.2.2.7. Outside the United States, to assess United States persons as potential sources of assistance to foreign intelligence and counterintelligence activities.

C10.4. DISCLOSURE REQUIREMENT

C10.4.1. Disclosure of the intelligence affiliation of an employee of a DoD intelligence component shall be made to an executive officer of the organization in question, or to an official in charge of membership, attendance, or the records of the organization concerned.

C10.4.2. Disclosure may be made by the DoD intelligence component involved, an authorized DoD official, or by another component of the Intelligence Community that is otherwise authorized to take such action on behalf of the DoD intelligence component concerned.

C11. CHAPTER 11: PROCEDURE 11. CONTRACTING FOR GOODS AND SERVICES

C11.1. APPLICABILITY

This procedure applies to contracting or other arrangements with United States persons for the procurement of goods and services by DoD intelligence components within the United States. This procedure does not apply to contracting with government entities, or to the enrollment of individual students in academic institutions. The latter situation is governed by Procedure 10.

C11.2. PROCEDURES

C11.2.1. Contracts with Academic Institutions

DoD intelligence components may enter into a contract for goods or services with an academic institution only if prior to the making of the contract, the intelligence component has disclosed to appropriate officials of the academic institution the fact of sponsorship by a DoD intelligence component.

C11.2.2. Contracts with Commercial Organizations, Private Institutions, and Individuals

Contracting by or for a DoD intelligence component with commercial organizations, private institutions, or private individuals within the United States may be done without revealing the sponsorship of the intelligence component if:

- C11.2.2.1. The contract is for published material available to the general public or for routine goods or services necessary for the support of approved activities, such as credit cards, car rentals, travel, lodging, meals, rental of office space or apartments, and other items incident to approved activities; or
- C11.2.2.2. There is a written determination by the Secretary or the Under Secretary of a Military Department, the Director of the National Security Agency, the Director of the Defense Intelligence Agency, or the Deputy Under Secretary of Defense (Policy) that the sponsorship of a DoD intelligence component must be concealed to protect the activities of the DoD intelligence component concerned.

C11.3. EFFECT OF NONCOMPLIANCE

No contract shall be void or voidable for failure to comply with this procedure.

C12. CHAPTER 12: PROCEDURE 12. PROVISION OF ASSISTANCE TO LAW ENFORCEMENT AUTHORITIES

C12.1. APPLICABILITY

This procedure applies to the provision of assistance by DoD intelligence components to law enforcement authorities. It incorporates the specific limitations on such assistance contained in E.O. 12333 (reference (a)), together with the general limitations and approval requirements of DoD Directive 5525.5 (reference (i)).

C12.2. PROCEDURES

C12.2.1. Cooperation with Law Enforcement Authorities

Consistent with the limitations contained in DoD Directive 5525.5 (reference (i)), and paragraph C12.2.2., below, DoD intelligence components are authorized to cooperate with law enforcement authorities for the purpose of:

- C12.2.1.1. Investigating or preventing clandestine intelligence activities by foreign powers, international narcotics activities, or international terrorist activities;
- C12.2.1.2. Protecting DoD employees, information, property, and facilities; and
- C12.2.1.3. Preventing, detecting, or investigating other violations of law.

C12.2.2. Types of Permissible Assistance

DoD intelligence components may provide the following types of assistance to law enforcement authorities:

- C12.2.2.1. Incidentally acquired information reasonably believed to indicate a violation of Federal law shall be provided in accordance with the procedures adopted pursuant to section 1.7(a) of E.O. 12333 (reference (a));
- C12.2.2.2. Incidentally acquired information reasonably believed to indicate a violation of State, local, or foreign law may be provided in accordance with procedures adopted by the Heads of DoD Components;
- C12.2.2.3. Specialized equipment and facilities may be provided to Federal law enforcement authorities, and, when lives are endangered, to State and local law enforcement authorities, provided such assistance is consistent with, and has been approved by an official authorized pursuant to, Enclosure 3 of DoD Directive 5525.5 (reference (i)); and
- C12.2.2.4. Personnel who are employees of DoD intelligence components may be assigned to assist Federal law enforcement authorities, and, when lives are endangered, State and local law enforcement authorities, provided such use is consistent with, and has been approved by an official authorized pursuant to, Enclosure 4 of DoD Directive 5525.5 (reference (i)). Such official shall ensure that the General Counsel of the providing DoD Component concurs in such use.

- C12.2.2.5. Assistance may be rendered to law enforcement agencies and security services of foreign governments or international organizations in accordance with established policy and applicable Status of Forces Agreements; provided, that DoD intelligence components may not request or participate in activities of such agencies undertaken against United States persons that would not be permitted such components under these procedures.

C13. CHAPTER 13: PROCEDURE 13. EXPERIMENTATION ON HUMAN SUBJECTS FOR INTELLIGENCE PURPOSES

C13.1. APPLICABILITY

This procedure applies to experimentation on human subjects if such experimentation is conducted by or on behalf of a DoD intelligence component. This procedure does not apply to experimentation on animal subjects.

C13.2. EXPLANATION OF UNDEFINED TERMS

- C13.2.1. Experimentation in this context means any research or testing activity involving human subjects that may expose such subjects to the possibility of permanent or temporary injury (including physical or psychological damage and damage to the reputation of such persons) beyond the risks of injury to which such subjects are ordinarily exposed in their daily lives.
- C13.2.2. Experimentation is conducted on behalf of a DoD intelligence component if it is conducted under contract to that component or to another DoD Component for the benefit of the intelligence component or at the request of such a component regardless of the existence of a contractual relationship.
- C13.2.3. Human subjects in this context includes any person whether or not such person is a United States person.

C13.3. PROCEDURES

- C13.3.1. Experimentation on human subjects conducted by or on behalf of a DoD intelligence component may be undertaken only with the informed consent of the subject, in accordance with guidelines issued by the Department of Health and Human Services, setting out conditions that safeguard the welfare of such subjects.
- C13.3.2. DoD intelligence components may not engage in or contract for experimentation on human subjects without approval of the Secretary or Deputy Secretary of Defense, or the Secretary or Under Secretary of a Military Department, as appropriate.

C14. CHAPTER 14: PROCEDURE 14. EMPLOYEE CONDUCT

C14.1. APPLICABILITY

This procedure sets forth the responsibilities of employees of DoD intelligence components to conduct themselves in accordance with this Regulation and other applicable policy. It also provides that DoD intelligence components shall ensure, as appropriate, that these policies and guidelines are made known to their employees.

C14.2. PROCEDURES

C14.2.1. Employee Responsibilities

Employees shall conduct intelligence activities only pursuant to, and in accordance with, Executive Order 12333 (reference (a)) and this Regulation. In conducting such activities, employees shall not exceed the authorities granted the employing DoD intelligence component by law; Executive order, including E.O. 12333 (reference (a)), and applicable DoD Directives.

C14.2.2. Familiarity With Restrictions

- C14.2.2.1. Each DoD intelligence component shall familiarize its personnel with the provisions of E.O. 12333 (reference (a)), this Regulation, and any instructions implementing this Regulation that apply to the operations and activities of such component. At a minimum, such familiarization shall contain:
    - C14.2.2.1.1. Applicable portions of Procedures 1 through 4;
    - C14.2.2.1.2. A summary of other procedures that pertains to collection techniques that are, or may be, employed by the DoD intelligence component concerned; and
    - C14.2.2.1.3. A statement of individual employee reporting responsibility under Procedure 15.
- C14.2.2.2. The Assistant to the Secretary of Defense (Intelligence Oversight) (ATSD(IQ)) and each Inspector General responsible for a DoD intelligence component shall ensure, as part of their inspections, that procedures are in effect that will achieve the objectives set forth in subparagraph C14.2.2.1., above.

C14.2.3. Responsibilities of the Heads of DoD Components

The Heads of DoD Components that constitute, or contain, DoD intelligence components shall:

- C14.2.3.1. Ensure that all proposals for intelligence activities that may be unlawful, in whole or in part, or may be contrary to applicable Executive Branch or DoD policy are referred to the General Counsel responsible for such component.

- C14.2.3.2. Ensure that no adverse action is taken against any employee because the employee reports activities pursuant to Procedure 15.
- C14.2.3.3. Impose such sanctions as may be appropriate upon any employee who violates the provisions of this Regulation or any instruction promulgated thereunder.
- C14.2.3.4. In any case involving serious or continuing breaches of security by either DoD or non-DoD employees, recommend to the Secretary of Defense appropriate investigative actions.
- C14.2.3.5. Ensure that the General Counsel and Inspector General with responsibility for the component, as well as the General Counsel, DoD, and the ATSD(IO), have access to all information concerning the intelligence activities of that component necessary to perform their oversight responsibilities.
- C14.2.3.6. Ensure that employees cooperate fully with the Intelligence Oversight Board and its representatives.

C15. CHAPTER 15: PROCEDURE 15. IDENTIFYING, INVESTIGATING, AND REPORTING QUSTIONABLE ACTIVITIES

C15.1. APPLICABILITY

This procedure provides for the identification, investigation, and reporting of questionable intelligence activities.

C15.2. EXPLANATION OF UNDEFINED TERMS

C15.2.1. "Questionable Activity"

The term "questionable activity," as used herein, refers to any conduct that constitutes, or is related to, an intelligence activity that may violate the law, any Executive order or Presidential directive, including E.O. 12333 (reference (a)), or applicable DoD policy, including this Regulation.

C15.2.2. "General Counsel" and "Inspector General"

The terms "General Counsel" and "Inspector General," as used herein, refer, unless otherwise specified, to any General Counsel or Inspector General with responsibility for one or more DoD intelligence components. Unless otherwise indicated, the term "Inspector General" shall also include the ATSD(IO).

C15.3. PROCEDURES

C15.3.1. Identification

- C15.3.1.1. Each employee shall report any questionable activity to the General Counsel or Inspector General for the DoD intelligence component concerned, or to the General Counsel, DoD, or ATSD(IO).
- C15.3.1.2. Inspectors General, as part of their inspection of DoD intelligence components, and General Counsels, as part of their oversight responsibilities shall seek to determine if such components are involved in any questionable activities. If such activities have been or are being undertaken, the matter shall be investigated under paragraph C15.3.2., below. If such activities have been undertaken, but were not reported, the Inspector General shall also ascertain the reason for such failure and recommend appropriate corrective action.
- C15.3.1.3. Inspectors General, as part of their oversight responsibilities, shall, as appropriate, ascertain whether any organizations, staffs, or offices within their respective jurisdictions, but not otherwise specifically identified as DoD intelligence components, are being used for foreign intelligence or counterintelligence purposes to which Part 2 of E.O. 12333 (reference (a)), applies, and, if so, shall ensure the activities of such components are in compliance with this Regulation and applicable DoD policy.
- C15.3.1.4. Inspectors General, as part of their inspection of DoD intelligence components, shall ensure that procedures exist within such

components for the reporting of questionable activities, and that employees of such components are aware of their responsibilities to report such activities.

C15.3.2. Investigation

- C15.3.2.1. Each report of a questionable activity shall be investigated to the extent necessary to determine the facts and assess whether the activity is legal and is consistent with applicable policy.
- C15.3.2.2. When appropriate, questionable activities reported to a General Counsel shall be referred to the corresponding Inspector General for investigation, and if reported to an Inspector General, shall be referred to the corresponding General Counsel to determine whether the activity is legal and consistent with applicable policy. Reports made to the DoD General Counsel or the ATSD(IO) may be referred, after consultation between these officials, to the appropriate Inspector General and General Counsel for investigation and evaluation.
- C15.3.2.3. Investigations shall be conducted expeditiously. The officials responsible for these investigations may, in accordance with established procedures, obtain assistance from within the component concerned, or from other DoD Components, when necessary, to complete such investigations in a timely manner.
- C15.3.2.4. To complete such investigations, General Counsels and Inspectors General shall have access to all relevant information regardless of classification or compartmentation.

C15.3.3. Reports

- C15.3.3.1. Each General Counsel and Inspector General shall report immediately to the General Counsel, DoD, and the ATSD(IO) questionable activities of a serious nature.
- C15.3.3.2. Each General Counsel and Inspector General shall submit to the ATSD(IO) a quarterly report describing those activities that come to their attention during the quarter reasonably believed to be illegal or contrary to Executive order or Presidential directive, or applicable DoD policy; and actions taken with respect to such activities. The reports shall also include significant oversight activities undertaken during the quarter and any suggestions for improvements in the oversight system. Separate, joint, or consolidated reports may be submitted. These reports should be prepared in accordance with DoD Directive 5000.11 (reference (j)).
- C15.3.3.3. All reports made pursuant to subparagraphs C15.3.3.1., and C15.3.3.2., above, which involve a possible violation of Federal criminal law shall be considered by the General Counsel concerned in accordance with the procedures adopted pursuant to section 1.7(a) of E.O. 12333 (reference (a)).

- C15.3.3.4. The General Counsel, DoD, and the ATSD(IO) may review the findings of other General Counsels and Inspectors General with respect to questionable activities.
- C15.3.3.5. The ATSD(IO) and the General Counsel, DoD, shall report in a timely manner to the White House Intelligence Oversight Board all activities that come to their attention that are reasonably believed to be illegal or contrary to Executive order or Presidential directive. They will also advise appropriate officials of the Office of the Secretary of Defense of such activities.
- C15.3.3.6. These reporting requirements are exempt from format approval and licensing in accordance with paragraph VII.G. of Enclosure 3 to DoD Directive 5000.19 (reference (k)).

Department of Defense Directive 5240.01

As Amended Through January 1, 2010

U.S. Dep't of Defense, Directive No. 5240.01, DoD Intelligence Activities (Aug. 2007), *available at* http://www.intelligencelaw.com/library/admin/html/dodd_5240-01_aug-2007.html.

Table of Contents

SUBJECT: DoD Intelligence Activities

References:

- DoD Directive 5240.1, "DoD Intelligence Activities," April 25, 1988 (hereby canceled)
- DoD Directive 5143.01, "Under Secretary of Defense for Intelligence," November 23, 2005
- Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended by Executive Order 13284, January 23, 2003, and Executive Order 13355, August 27, 2004
- Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," October 25, 2005
- through (k), see Enclosure l

1. REISSUANCE AND PURPOSE

This Directive:

- Reissues Reference (a) and implements References (b), (c), and (d); section 188 of Public Law 108-458 (Reference (e)); Executive Order 12863 (Reference (f)); and chapter 36 of title 50, United States Code (Reference (g)).
- Updates policy and provides direction for DoD intelligence activities.
- Shall be the primary authority used as guidance by the Defense Intelligence Components and those performing an intelligence or

counterintelligence (CI) function to collect, process, retain, or disseminate information concerning U.S. persons.
- Continues to authorize the publication of DoD 5240.1-R (Reference (h)).

2. APPLICABILITY AND SCOPE

This Directive:

- 2.1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").
- 2.2. Applies to all intelligence activities conducted by the DoD Components.
- 2.3. Does not apply to authorized law enforcement activities carried out by the Defense Intelligence Components, or to individuals executing law enforcement missions while assigned to the Defense Intelligence Components.

3. DEFINITIONS

Terms used in this Directive are defined in Enclosure 2.

4. POLICY

It is DoD policy that:

- 4.1. All DoD intelligence and CI activities shall be carried out pursuant to the authorities and restrictions of the U.S. Constitution, applicable law, Reference (c), the policies and procedures authorized herein, and other relevant DoD policies authorized by Reference (b). Special emphasis shall be given to the protection of the constitutional rights and privacy of U.S. persons.
- 4.2. DoD intelligence and CI activities shall conform to U.S. law and Presidential guidance concerning the authorities and responsibilities of the Director of National Intelligence (DNI).
- 4.3. Defense Intelligence and CI shall be the all-source information collection, analysis, sharing, and dissemination capability derived from intelligence and CI activities, operations, and campaign plans, provided to national and defense decision makers and warfighters for military planning and operations.
- 4.4. Defense Intelligence shall provide accurate and timely warning of threats and of foreign capabilities and intent to national and defense decision makers to allow for consideration of the widest range of options. While Defense Intelligence must be timely, it also must be substantive, thorough, contextual, and useful in form and format.
- 4.5. Consistent with the need to protect intelligence sources and methods and the provisions of Director of Central Intelligence Directive 8/1

(Reference (i)), the Defense Intelligence and CI Components have an affirmative responsibility to share collected and stored information, data, and resulting analysis with other Defense Intelligence and CI Components, the national Intelligence Community (IC), other relevant Federal agencies, and civilian law enforcement officials, as appropriate. This also applies to the exchange and sharing of terrorism-related information pursuant to Reference (d). Information sharing shall adhere to the requirements and restrictions imposed by Federal law, Executive order, and DoD and DNI policies.

    - 4.5.1. The Defense Intelligence and CI Components shall share collected or stored information in a manner consistent with both the need to protect sources and methods and the need to enable the Defense Intelligence and DoD Components, other Government agencies, and the Intelligence Community, as appropriate, to accomplish their missions and responsibilities.
    - 4.5.2. The broadest possible sharing of intelligence with coalition and approved partner countries shall be accomplished unless otherwise precluded from release by law, explicit direction, or policy.
    - 4.5.3. Original classifiers shall draft intelligence products with a presumption of release and in such a manner as to allow the widest dissemination to allies, coalitions, and international organizations.

- 4.6. No Defense Intelligence or CI Component shall request any person or entity to undertake unauthorized activities on behalf of the Defense Intelligence or CI Component. No Defense Intelligence or CI Component shall request any person or entity to undertake intelligence activities on behalf of the Defense Intelligence or CI Component that do not follow the procedures described in Reference (h). The collection techniques described in Reference (h) shall be employed only to perform intelligence or CI functions assigned to the Defense Intelligence Component concerned. Use of such techniques to collect information about U.S. persons shall be limited to the least intrusive means feasible and shall not violate law, Executive order, Presidential guidance, or DoD or DNI policy.
- 4.7. The Defense Intelligence and CI Components and their employees shall report all intelligence or CI activities that may violate law, Executive order, Presidential directive, or applicable DoD policy through the Component chain of command to the Inspector General or General Counsel responsible for the Defense Intelligence Component concerned, or to the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)).
- 4.8. The Defense Intelligence Components shall only conduct, or provide support for the conduct of, covert activities in times of war declared by Congress, during a period covered by a report from the President to Congress consistent with sections 1541-1548 of Reference (g), or when

such actions have been approved by the President and directed by the Secretary of Defense.

- 4.9. Under no circumstances shall any DoD Component or DoD employee engage in, or conspire to engage in, assassination.

5. RESPONSIBILITIES

- 5.1. The Under Secretary of Defense for Intelligence (USD(I)), according to Reference (b), shall provide overall policy guidance for the conduct of DoD intelligence, CI, security, and intelligence-related activities. Pursuant to Reference (b), the USD(I) shall:
    - 5.1.1. Serve as the focal point for the Secretary of Defense, according to the responsibilities and functions prescribed herein, with other U.S. Government entities and agencies, including the National Security Council, the DNI, the Homeland Security Council, the Department of the Treasury, the Department of State, the Department of Justice, and the Department of Homeland Security as well as State agencies, the IC, and Congress.
    - 5.1.2. Serve as the focal point for the Secretary of Defense, according to the responsibilities and functions prescribed herein, with foreign governments, international organizations, and non-governmental organizations.
    - 5.1.3. Promote coordination, cooperation, information sharing, and crossservice management of intelligence, CI, security, and related programs within the Department of Defense and between the Department and other Federal agencies.
    - 5.1.4. Provide oversight and policy guidance on sensitive intelligence activities; serve as the DoD lead for Departmental participation in all such activities.
- 5.2. The Department of Defense General Counsel shall:
    - 5.2.1. Serve as the focal point for contact with, and reporting to, the Attorney General regarding legal matters arising under this Directive.
    - 5.2.2. Interpret this Directive and Reference (h), as required.
- 5.3. The ATSD(IO) shall serve as the focal point for all contacts with the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board pursuant to Reference (f), and shall perform the responsibilities assigned in DoD Directive 5148.11 (Reference (j)).
- 5.4. The Secretaries of the Military Departments with IC elements shall:
    - 5.4.1. Organize, staff, train, and equip the intelligence assets of the Military Departments, including CI, signals intelligence, geospatial intelligence, measurement and signatures intelligence, and human intelligence assets, to support operational forces, national-level policy-makers, and the acquisition community.

- 5.4.2. Develop intelligence capabilities including interoperable and compatible systems, databases, and procedures for joint operational forces according to DoD guidance; Combatant Commander and Director, Defense Intelligence Agency, requirements; the Defense Intelligence Information System Network-Centric Architecture; and the Joint Technical Architecture.
- 5.4.3. Fulfill assigned Defense Intelligence Analysis Program responsibilities, both national level and Military Department-unique, for national intelligence activities in support of national and DoD entities through timely, tailored, all-source intelligence tasking, collection, processing/exploitation, analysis/production, and dissemination/integration.

6. EFFECTIVE DATE

This Directive is effective immediately.

Enclosures – 2

E1. References, continued
E2. Definitions

E1. ENCLOSURE 1 - REFERENCES, continued

- (e) Section 188 of Public Law 108-458, "Intelligence Reform and Terrorism Prevention Act of 2004," December 17, 2004
- (f) Executive Order 12863, "President's Foreign Intelligence Advisory Board," September 13, 1993, as amended by Executive Order 13070, December 15, 1997; Executive Order 13301, May 14, 2003; and Executive Order 13376, April 13, 2005
- (g) Chapter 36 and sections 401a(2), 413, and 1541-1548 of title 50, United State Code
- (h) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 11, 1982
- Director of Central Intelligence Directive 8/1, "Intelligence Community Policy on Intelligence Information Sharing," June 4, 2004
- (j) DoD Directive 5148.11, "Assistant to the Secretary of Defense (Intelligence Oversight)," May 21, 2004
- (k) Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms," as amended

E2. ENCLOSURE 2 - DEFINITIONS

E2.1. All-Source Analysis

An intelligence activity involving the integration, evaluation, and interpretation of information from all available data sources and types, to include human intelligence, signals intelligence, geospatial intelligence, measurement and signature intelligence, and open source intelligence.

E2.2. CI

Defined in Joint Publication 1-02 (Reference (k)).

E2.3. Defense CI Components

Defined in Reference (b).

E2.4. Defense Intelligence

Defined in Reference (b).

E2.5. Defense Intelligence Components

Defined in Reference (b).

E2.6. Foreign Intelligence

Defined in section 401a(2) of Reference (g).

E2.7. Intelligence Activities

The collection, analysis, production, and dissemination of foreign intelligence and CI pursuant to References (b) and (c).

E2.8. National Intelligence

Defined in Reference (b).

E2.9. Covert Action

Defined in section 413 of Reference (g).

E2.10. U.S. Person

Defined in Reference (c).

The Attorney General's Guidelines for Domestic FBI Operations

As Amended Through January 1, 2010

U.S. Dep't of Justice, *The Attorney General's Guidelines for Domestic FBI Operations*, § VII (A) (Sept. 29, 2008), *available at* http://www.intelligencelaw.com/library/admin/html/ag_guidelines_2008.html.

Table of Contents

PREAMBLE

These Guidelines are issued under the authority of the Attorney General as provided in sections 509, 510, 533, and 534 of title 28, United States Code, and Executive Order 12333. They apply to domestic investigative activities of the Federal Bureau of Investigation (FBI) and other activities as provided herein.

INTRODUCTION

As the primary investigative agency of the federal government, the Federal Bureau of Investigation (FBI) has the authority and responsibility to investigate all violations of federal law that are not exclusively assigned to another federal agency. The FBI is further vested by law and by Presidential directives with the primary role in carrying out investigations within the United States of threats to the national security. This includes the lead domestic role in investigating international terrorist threats to the United States, and in conducting counterintelligence activities to meet foreign entities' espionage and intelligence efforts directed against the United States. The FBI is also vested with important functions in collecting foreign intelligence as a member agency of the U.S. Intelligence Community. The FBI accordingly plays crucial roles in the enforcement of federal law and the proper administration of justice in the United

States, in the protection of the national security, and in obtaining information needed by the United States for the conduct of its foreign affairs. These roles reflect the wide range of the FBI's current responsibilities and obligations, which require the FBI to be both an agency that effectively detects, investigates, and prevents crimes, and an agency that effectively protects the national security and collects intelligence.

The general objective of these Guidelines is the full utilization of all authorities and investigative methods, consistent with the Constitution and laws of the United States, to protect the United States and its people from terrorism and other threats to the national security, to protect the United States and its people from victimization by all crimes in violation of federal law, and to further the foreign intelligence objectives of the United States. At the same time, it is axiomatic that the FBI must conduct its investigations and other activities in a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding people. The purpose of these Guidelines, therefore, is to establish consistent policy in such matters. They will enable the FBI to perform its duties with effectiveness, certainty, and confidence, and will provide the American people with a firm assurance that the FBI is acting properly under the law.

The issuance of these Guidelines represents the culmination of the historical evolution of the FBI and the policies governing its domestic operations subsequent to the September 11, 2001, terrorist attacks on the United States. Reflecting decisions and directives of the President and the Attorney General, inquiries and enactments of Congress, and the conclusions of national commissions, it was recognized that the FBI's functions needed to be expanded and better integrated to meet contemporary realities:

> [Continuing coordination .. .is necessary to optimize the FBI's performance in both national security and criminal investigations . . . . [The] new reality requires first that the FBI and other agencies do a better job of gathering intelligence inside the United States, and second that we eliminate the remnants of the old "wall" between foreign intelligence and domestic law enforcement. Both tasks must be accomplished without sacrificing our domestic liberties and the rule of law, and both depend on building a very different FBI from the one we had on September 10,2001. (Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction 466,452 (2005).)

In line with these objectives, the FBI has reorganized and reoriented its programs and missions, and the guidelines issued by the Attorney General for FBI operations have been extensively revised over the past several years. Nevertheless, the principal directives of the Attorney General governing the FBI's conduct of criminal investigations, national security investigations, and foreign intelligence collection have persisted as separate documents involving different

standards and procedures for comparable activities. These Guidelines effect a more complete integration and harmonization of standards, thereby providing the FBI and other affected Justice Department components with clearer, more consistent, and more accessible guidance for their activities, and making available to the public in a single document the basic body of rules for the FBI's domestic operations.

These Guidelines also incorporate effective oversight measures involving many Department of Justice and FBI components, which have been adopted to ensure that all FBI activities are conducted in a manner consistent with law and policy.

The broad operational areas addressed by these Guidelines are the FBI's conduct of investigative and intelligence gathering activities, including cooperation and coordination with other components and agencies in such activities, and the intelligence analysis and planning functions of the FBI.

A. FBI RESPONSIBILITIES—FEDERAL CRIMES, THREATS TO THE NATIONAL SECURITY, FOREIGN INTELLIGENCE

Part 11of these Guidelines authorizes the FBI to carry out investigations to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence. The major subject areas of information gathering activities under these Guidelines -federal crimes, threats to the national security, and foreign intelligence--are not distinct, but rather overlap extensively. For example, an investigation relating to international terrorism will invariably crosscut these areas because international terrorism is included under these Guidelines' definition of "threat to the national security," because international terrorism subject to investigation within the United States usually involves criminal acts that violate federal law, and because information relating to international terrorism also falls within the definition of "foreign intelligence." Likewise, counterintelligence activities relating to espionage are likely to concern matters that constitute threats to the national security, that implicate violations or potential violations of federal espionage laws, and that involve information falling under the definition of "foreign intelligence."

While some distinctions in the requirements and procedures for investigations are necessary in different subject areas, the general design of these Guidelines is to take a uniform approach wherever possible, thereby promoting certainty and consistency regarding the applicable standards and facilitating compliance with those standards. Hence, these Guidelines do not require that the FBI's information gathering activities be differentially labeled as "criminal investigations," "national security investigations," or "foreign intelligence collections," or that the categories of FBI personnel who carry out investigations be segregated from each other based on the subject areas in which they operate. Rather, all of the FBI's legal authorities are available for deployment in all cases to which they apply to protect the public from crimes and threats to the national

security and to further the United States' foreign intelligence objectives. In many cases, a single investigation will be supportable as an exercise of a number of these authorities -i.e., as an investigation of a federal crime or crimes, as an investigation of a threat to the national security, and/or as a collection of foreign intelligence.

1. Federal Crimes

The FBI has the authority to investigate all federal crimes that are not exclusively assigned to other agencies. In most ordinary criminal investigations, the immediate objectives include such matters as: determining whether a federal crime has occurred or is occurring, or if planning or preparation for such a crime is taking place; identifying, locating, and apprehending the perpetrators; and obtaining the evidence needed for prosecution. Hence, close cooperation and coordination with federal prosecutors in the United States Attorneys' Offices and the Justice Department litigating divisions are essential both to ensure that agents have the investigative tools and legal advice at their disposal for which prosecutorial assistance or approval is needed, and to ensure that investigations are conducted in a manner that will lead to successful prosecution. Provisions in many parts of these Guidelines establish procedures and requirements for such coordination.

2. Threats to the National Security

The FBI's authority to investigate threats to the national security derives from the executive order concerning U.S. intelligence activities, from delegations of functions by the Attorney General, and from various statutory sources. See, e.g., E.O. 12333; 50 U.S.C. 401 et seq.; 50 U.S.C. 1801 et seq. These Guidelines (Part VII.S) specifically define threats to the national security to mean: international terrorism; espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the Attorney General, consistent with Executive Order 12333 or any successor order.

Activities within the definition of "threat to the national security" that are subject to investigation under these Guidelines commonly involve violations (or potential violations) of federal criminal laws. Hence, investigations of such threats may constitute an exercise both of the FBI's criminal investigation authority and of the FBI's authority to investigate threats to the national security. As with criminal investigations generally, detecting and solving the crimes, and eventually arresting and prosecuting the perpetrators, are likely to be among the objectives of investigations relating to threats to the national security. But these investigations also often serve important purposes outside the ambit of normal criminal investigation and prosecution, by providing the basis for, and informing decisions concerning, other measures needed to protect the national security. These measures may include, for example: excluding or removing persons involved in terrorism or espionage from the United States; recruitment of double agents; freezing assets of organizations that engage in or support terrorism;

securing targets of terrorism or espionage; providing threat information and warnings to other federal, state, local, and private agencies and entities; diplomatic or military actions; and actions by other intelligence agencies to counter international terrorism or other national security threats.

In line with this broad range of purposes, investigations of threats to the national security present special needs to coordinate with other Justice Department components, including particularly the Justice Department's National Security Division, and to share information and cooperate with other agencies with national security responsibilities, including other agencies of the U.S. Intelligence Community, the Department of Homeland Security, and relevant White House (including National Security Council and Homeland Security Council) agencies and entities. Various provisions in these Guidelines establish procedures and requirements to facilitate such coordination.

3. Foreign Intelligence

As with the investigation of threats to the national security, the FBI's authority to collect foreign intelligence derives from a mixture of administrative and statutory sources. See, e.g., E.O. 12333; 50 U.S.C. 401 et seq.; 50 U.S.C. 1801 et seq.; 28 U.S.C. 532 note (incorporating
P.L. 108-458 $5 2001-2003). These Guidelines (Part VI1.E) define foreign intelligence to mean "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists."

The FBI's foreign intelligence collection activities have been expanded by legislative and administrative reforms subsequent to the September 1 1,2001, terrorist attacks, reflecting the FBI's role as the primary collector of foreign intelligence within the United States, and the recognized imperative that the United States' foreign intelligence collection activities become more flexible, more proactive, and more efficient in order to protect the homeland and adequately inform the United States' crucial decisions in its dealings with the rest of the world:

> The collection of information is the foundation of everything that the Intelligence Community does. While successful collection cannot ensure a good analytical product, the failure to collect information . . . turns analysis into guesswork. And as our review demonstrates, the Intelligence Community's human and technical intelligence collection agencies have collected far too little information on many of the issues we care about most. (Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction 35 1 (2005).)

These Guidelines accordingly provide standards and procedures for the FBI's foreign intelligence collection activities that meet current needs and realities and optimize the FBI's ability to discharge its foreign intelligence collection functions.

The authority to collect foreign intelligence extends the sphere of the FBI's information gathering activities beyond federal crimes and threats to the national security, and permits the FBI to seek information regarding a broader range of matters relating to foreign powers, organizations, or persons that may be of interest to the conduct of the United States' foreign affairs. The FBI's role is central to the effective collection of foreign intelligence within the United States because the authorized domestic activities of other intelligence agencies are more constrained than those of the FBI under applicable statutes and Executive Order 12333. In collecting foreign intelligence, the FBI will generally be guided by nationally-determined intelligence requirements, including the National Intelligence Priorities Framework and the National HUMINT Collection Directives, or any successor directives issued under the authority of the Director of National Intelligence (DNI). As provided in Part VII.F of these Guidelines, foreign intelligence requirements may also be established by the President or Intelligence Community officials designated by the President, and by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General.

The general guidance of the FBI's foreign intelligence collection activities by DNI-authorized requirements does not, however, limit the FBI's authority to -conduct investigations supportable on the basis of its other authorities -to investigate federal crimes and threats to the national security -in areas in which the information sought also falls under the definition of foreign intelligence. The FBI conducts investigations of federal crimes and threats to the national security based on priorities and strategic objectives set by the Department of Justice and the FBI, independent of DNI-established foreign intelligence collection requirements.

Since the authority to collect foreign intelligence enables the FBI to obtain information pertinent to the United States' conduct of its foreign affairs, even if that information is not related to criminal activity or threats to the national security, the information so gathered may concern lawful activities. The FBI should accordingly operate openly and consensually with U.S. persons to the extent practicable when collecting foreign intelligence that does not concern criminal activities or threats to the national security.

B. THE FBI AS AN INTELLIGENCE AGENCY

The FBI is an intelligence agency as well as a law enforcement agency. Its basic functions accordingly extend beyond limited investigations of discrete matters, and include broader analytic and planning functions. The FBI's responsibilities in this area derive from various administrative and statutory sources. See, e.g., E.O. 12333; 28 U.S.C. 532 note (incorporating P.L. 108-458 $5 2001 -2003) and 534 note (incorporating P.L. 109-1 62 8 1 107). Enhancement of the FBI's intelligence analysis capabilities and functions has consistently been recognized as a key

priority in the legislative and administrative reform efforts following the September 1 1,2001, terrorist attacks:

> [Counterterrorism] strategy should . . . encompass specific efforts to . . . enhance the depth and quality of domestic intelligence collection and analysis . . . . [T]he FBI should strengthen and improve its domestic [intelligence] capability as fully and expeditiously as possible by immediately instituting measures to . . . significantly improve strategic analytical capabilities . . . . (Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11,2001, S. Rep. No. 351 & H.R. Rep. No. 792, 107th Cong., 2d Sess. 4-7 (2002) (errata print).)

> A "smart" government would integrate all sources of information to see the enemy as a whole. Integrated all-source analysis should also inform and shape strategies to collect more intelligence. . . . The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to "connect the dots." (Final Report of the National Commission on Terrorist Attacks Upon the United States 401,408 (2004).)

Part IV of these Guidelines accordingly authorizes the FBI to engage in intelligence analysis and planning, drawing on all lawful sources of information. The functions authorized under that Part include: (i) development of overviews and analyses concerning threats to and vulnerabilities of the United States and its interests, (ii) research and analysis to produce reports and assessments concerning matters relevant to investigative activities or other authorized FBI activities, and (iii) the operation of intelligence systems that facilitate and support investigations through the compilation and analysis of data and information on an ongoing basis.

C. OVERSIGHT

The activities authorized by these Guidelines must be conducted in a manner consistent with all applicable laws, regulations, and policies, including those protecting privacy and civil liberties. The Justice Department's National Security Division and the FBI's Inspection Division, Office of General Counsel, and Office of Integrity and Compliance, along with other components, share the responsibility to ensure that the Department meets these goals with respect to national security and foreign intelligence matters. In particular, the National Security Division's Oversight Section, in conjunction with the FBI's Office of General Counsel, is responsible for conducting regular reviews of all aspects of FBI national security and foreign intelligence activities. These reviews, conducted at FBI field offices and headquarter units, broadly examine such activities for compliance with these Guidelines and other applicable requirements.

Various features of these Guidelines facilitate the National Security Division's oversight functions. Relevant requirements and provisions include: (i) required notification by the FBI to the National Security Division concerning full investigations that involve foreign intelligence collection or investigation of United States persons in relation to threats of the national security,
(ii) annual reports by the FBI to the National Security Division concerning the FBI's foreign intelligence collection program, including information on the scope and nature of foreign intelligence collection activities in each FBI field office, and (iii) access by the National Security Division to information obtained by the FBI through national security or foreign intelligence activities and general authority for the Assistant Attorney General for National Security to obtain reports from the FBI concerning these activities.

Pursuant to these Guidelines, other Attorney General guidelines, and institutional assignments of responsibility within the Justice Department, additional Department components--including the Criminal Division, the United States Attorneys' Offices, and the Office of Privacy and Civil Liberties -are involved in the common endeavor with the FBI of ensuring that the activities of all Department components are lawful, appropriate, and ethical as well as effective. Examples include the involvement of both FBI and prosecutorial personnel in the review of undercover operations involving sensitive circumstances, notice requirements for investigations involving sensitive investigative matters (as defined in Part V1I.N of these Guidelines), and notice and oversight provisions for enterprise investigations, which may involve a broad examination of groups implicated in the gravest criminal and national security threats. These requirements and procedures help to ensure that the rule of law is respected in the Department's activities and that public confidence is maintained in these activities.

I. GENERAL AUTHORITIES AND PRINCIPLES

A. SCOPE

These Guidelines apply to investigative activities conducted by the FBI within the United States or outside the territories of all countries. They do not apply to investigative activities of the FBI in foreign countries, which are governed by the Attorney General's Guidelines for Extraterritorial FBI Operations.

B. GENERAL AUTHORITIES

1. The FBI is authorized to conduct investigations to detect, obtain information about, and prevent and protect against federal crimes and threats to the national security and to collect foreign intelligence, as provided in Part I1 of these Guidelines.
2. The FBI is authorized to provide investigative assistance to other federal agencies, state, local, or tribal agencies, and foreign agencies as provided in Part III of these Guidelines.
3. The FBI is authorized to conduct intelligence analysis and planning as provided in Part IV of these Guidelines.
4. The FBI is authorized to retain and share information obtained pursuant to these Guidelines as provided in Part VI of these Guidelines.

C.USE OF AUTHORITIES AND METHODS

1. Protection of the United States and Its People

The FBI shall fully utilize the authorities provided and the methods authorized by these Guidelines to protect the United States and its people from crimes in violation of federal law and threats to the national security, and to further the foreign intelligence objectives of the United States.

2. Choice of Methods

a. The conduct of investigations and other activities authorized by these Guidelines may present choices between the use of different investigative methods that are each operationally sound and effective, but that are more or less intrusive, considering such factors as the effect on the privacy and civil liberties of individuals and potential damage to reputation. The least intrusive method feasible is to be used in such situations. It is recognized, however, that the choice of methods is a matter of judgment. The FBI shall not hesitate to use any lawful method consistent with these Guidelines, even if intrusive, where the degree of intrusiveness is warranted in light of the seriousness of a criminal or national security threat or the strength of the information indicating its existence, or in light of the importance of foreign intelligence sought to the United States' interests. This point is to be particularly observed in investigations relating to terrorism.

b. United States persons shall be dealt with openly and consensually to the extent practicable when collecting foreign intelligence that does not concern criminal activities or threats to the national security.

3. Respect for Legal Rights

All activities under these Guidelines must have a valid purpose consistent with these Guidelines, and must be carried out in conformity with the Constitution and all applicable statutes, executive orders, Department of Justice regulations and policies, and Attorney General guidelines. These Guidelines do not authorize investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States. These Guidelines also do not authorize any conduct prohibited by the Guidance Regarding the Use of Race by Federal Law Enforcement Agencies.

4. Undisclosed Participation in Organizations

Undisclosed participation in organizations in activities under these Guidelines shall be conducted in accordance with FBI policy approved by the Attorney General.

5. Maintenance of Records under the Privacy Act

The Privacy Act restricts the maintenance of records relating to certain activities of individuals who are United States persons, with exceptions for circumstances in which the collection of such information is pertinent to and within the scope of an authorized law enforcement activity or is otherwise authorized by statute. 5 U.S.C. 552a(e)(7). Activities authorized by these Guidelines are authorized law enforcement activities or activities for which there is otherwise statutory authority for purposes of the Privacy Act. These Guidelines, however, do not provide an exhaustive enumeration of authorized FBI law enforcement activities or FBI activities for which there is otherwise statutory authority, and no restriction is implied with respect to such activities carried out by the FBI pursuant to other authorities. Further questions about the application of the Privacy Act to authorized activities of the FBI should be addressed to the FBI Office of the General Counsel, the FBI Privacy and Civil Liberties Unit, or the Department of Justice Office of Privacy and Civil Liberties.

D. NATURE AND APPLICATION OF THE GUIDELINES

1. Repealers

These Guidelines supersede the following guidelines, which are hereby repealed:

a. The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (May 30,2002) and all predecessor guidelines thereto.
b. The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (October 3 1,2003) and all predecessor guidelines thereto.

c. The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence (November 29, 2006).
d. The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations (August 8, 1988).
e. The Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest (April 5, 1976).

2. Status as Internal Guidance

These Guidelines are set forth solely for the purpose of internal Department of Justice guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable by law by any party in any matter, civil or criminal, nor do they place any limitation on otherwise lawful investigative and litigative prerogatives of the Department of Justice.

3. Departures from the Guidelines

Departures from these Guidelines must be approved by the Director of the FBI, by the Deputy Director of the FBI, or by an Executive Assistant Director designated by the Director. If a departure is necessary without such prior approval because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, the Director, the Deputy Director, or a designated Executive Assistant Director shall be notified as soon thereafter as practicable. The FBI shall provide timely written notice of departures from these Guidelines to the Criminal Division and the National Security Division, and those divisions shall notify the Attorney General and the Deputy Attorney General. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

4. Other Activities Not Limited

These Guidelines apply to FBI activities as provided herein and do not limit other authorized activities of the FBI, such as the FBI's responsibilities to conduct background checks and inquiries concerning applicants and employees under federal personnel security programs, the FBI's maintenance and operation of national criminal records systems and preparation of national crime statistics, and the forensic assistance and administration functions of the FBI Laboratory.

II. INVESTIGATIONS AND INTELLIGENCE GATHERING

This Part of the Guidelines authorizes the FBI to conduct investigations to detect, obtain information about, and prevent and protect against federal crimes and threats to the national security and to collect foreign intelligence.

When an authorized purpose exists, the focus of activities authorized by this Part may be whatever the circumstances warrant. The subject of such an activity may be, for example, a particular crime or threatened crime; conduct constituting a threat to the national security; an individual, group, or organization that may be involved in criminal or national security- threatening conduct; or a topical matter of foreign intelligence interest.

Investigations may also be undertaken for protective purposes in relation to individuals, groups, or other entities that may be targeted for criminal victimization or acquisition, or for terrorist attack or other depredations by the enemies of the United States. For example, the participation of the FBI in special events management, in relation to public events or other activities whose character may make them attractive targets for terrorist attack, is an authorized exercise of the authorities conveyed by these Guidelines. Likewise, FBI counterintelligence activities directed to identifying and securing facilities, personnel, or information that may be targeted for infiltration, recruitment, or acquisition by foreign intelligence services are authorized exercises of the authorities conveyed by these Guidelines.

The identification and recruitment of human sources—who may be able to provide or obtain information relating to criminal activities, information relating to terrorism, espionage, or other threats to the national security, or information relating to matters of foreign intelligence interest—is also critical to the effectiveness of the FBI's law enforcement, national security, and intelligence programs, and activities undertaken for this purpose are authorized and encouraged.

The scope of authorized activities under this Part is not limited to "investigation" in a narrow sense, such as solving particular cases or obtaining evidence for use in particular criminal prosecutions. Rather, these activities also provide critical information needed for broader analytic and intelligence purposes to facilitate the solution and prevention of crime, protect the national security, and further foreign intelligence objectives. These purposes include use of the information in intelligence analysis and planning under Part IV, and dissemination of the information to other law enforcement, Intelligence Community, and White House agencies under Part VI. Information obtained at all stages of investigative activity is accordingly to be retained and disseminated for these purposes as

provided in these Guidelines, or in FBI policy consistent with these Guidelines, regardless of whether it furthers investigative objectives in a narrower or more immediate sense.

In the course of activities under these Guidelines, the FBI may incidentally obtain information relating to matters outside of its areas of primary investigative responsibility. For example, information relating to violations of state or local law or foreign law may be incidentally obtained in the course of investigating federal crimes or threats to the national security or in collecting foreign intelligence. These Guidelines do not bar the acquisition of such information in the course of authorized investigative activities, the retention of such information, or its dissemination as appropriate to the responsible authorities in other agencies or jurisdictions. Part VI of these Guidelines includes specific authorizations and requirements for sharing such information with relevant agencies and officials.

This Part authorizes different levels of information gathering activity, which afford the FBI flexibility, under appropriate standards and procedures, to adapt the methods utilized and the information sought to the nature of the matter under investigation and the character of the information supporting the need for investigation.

Assessments, authorized by Subpart A of this Part, require an authorized purpose but not any particular factual predication. For example, to carry out its central mission of preventing the commission of terrorist acts against the United States and its people, the FBI must proactively draw on available sources of information to identify terrorist threats and activities. It cannot be content to wait for leads to come in through the actions of others, but rather must be vigilant in detecting terrorist activities to the full extent permitted by law, with an eye towards early intervention and prevention of acts of terrorism before they occur. Likewise, in the exercise of its protective functions, the FBI is not constrained to wait until information is received indicating that a particular event, activity, or facility has drawn the attention of those who would threaten the national security. Rather, the FBI must take the initiative to secure and protect activities and entities whose character may make them attractive targets for terrorism or espionage. The proactive investigative authority conveyed in assessments is designed for, and may be utilized by, the FBI in the discharge of these responsibilities. For example, assessments may be conducted as part of the FBI's special events management activities.

More broadly, detecting and interrupting criminal activities at their early stages, and preventing crimes from occurring in the first place, is preferable to allowing criminal plots and activities to come to fruition. Hence, assessments may be undertaken proactively with such objectives as detecting criminal activities; obtaining information on individuals, groups, or organizations of possible investigative interest, either because they may be involved in criminal or national security-threatening activities or because they may be targeted for attack or

victimization by such activities; and identifying and assessing individuals who may have value as human sources. For example, assessment activities may involve proactively surfing the Internet to find publicly accessible websites and services through which recruitment by terrorist organizations and promotion of terrorist crimes is openly taking place; through which child pornography is advertised and traded; through which efforts are made by sexual predators to lure children for purposes of sexual abuse; or through which fraudulent schemes are perpetrated against the public.

The methods authorized in assessments are generally those of relatively low intrusiveness, such as obtaining publicly available information, checking government records, and requesting information from members of the public. These Guidelines do not impose supervisory approval requirements in assessments, given the types of techniques that are authorized at this stage (e.g., perusing the Internet for publicly available information). However, FBI policy will prescribe supervisory approval requirements for certain assessments, considering such matters as the purpose of the assessment and the methods being utilized.

Beyond the proactive information gathering functions described above, assessments may be used when allegations or other information concerning crimes or threats to the national security is received or obtained, and the matter can be checked out or resolved through the relatively non-intrusive methods authorized in assessments. The checking of investigative leads in this manner can avoid the need to proceed to more formal levels of investigative activity, if the results of an assessment indicate that further investigation is not warranted.

Subpart B of this Part authorizes a second level of investigative activity, predicated investigations. The purposes or objectives of predicated investigations are essentially the same as those of assessments, but predication as provided in these Guidelines is needed -generally, allegations, reports, facts or circumstances indicative of possible criminal or national security- threatening activity, or the potential for acquiring information responsive to foreign intelligence requirements -and supervisory approval must be obtained, to initiate predicated investigations. Corresponding to the stronger predication and approval requirements, all lawful methods may be used in predicated investigations. A classified directive provides further specification concerning circumstances supporting certain predicated investigations.

Predicated investigations that concern federal crimes or threats to the national security are subdivided into preliminary investigations and full investigations. Preliminary investigations may be initiated on the basis of any allegation or information indicative of possible criminal or national security-threatening activity, but more substantial factual predication is required for full investigations. While time limits are set for the completion of preliminary

investigations, full investigations may be pursued without preset limits on their duration.

The final investigative category under this Part of the Guidelines is enterprise investigations, authorized by Subpart C, which permit a general examination of the structure, scope, and nature of certain groups and organizations. Enterprise investigations are a type of full investigations. Hence, they are subject to the purpose, approval, and predication requirements that apply to full investigations, and all lawful methods may be used in carrying them out. The distinctive characteristic of enterprise investigations is that they concern groups or organizations that may be involved in the most serious criminal or national security threats to the public -generally, patterns of racketeering activity, terrorism or other threats to the national security, or the commission of offenses characteristically involved in terrorism as described in 18 U.S.C. 2332b(g)(5)(B). A broad examination of the characteristics of groups satisfying these criteria is authorized in enterprise investigations, including any relationship of the group to a foreign power, its size and composition, its geographic dimensions and finances, its past acts and goals, and its capacity for harm.

A. ASSESSMENTS

1. Purposes

Assessments may be carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence.

2. Approval

The conduct of assessments is subject to any supervisory approval requirements prescribed by FBI policy.

3. Authorized Activities

Activities that may be carried out for the purposes described in paragraph 1 in an assessment include:

a. seeking information, proactively or in response to investigative leads, relating to:
    i. activities constituting violations of federal criminal law or threats to the national security,
    ii. the involvement or role of individuals, groups, or organizations in such activities; or
    iii. matters of foreign intelligence interest responsive to foreign intelligence requirements;
b. identifying and obtaining information about potential targets of or vulnerabilities to criminal activities in violation of federal law or threats to the national security;
c. seeking information to identify potential human sources, assess the suitability, credibility, or value of individuals as human sources, validate

human sources, or maintain the cover or credibility of human sources, who may be able to provide or obtain information relating to criminal activities in violation of federal law, threats to the national security, or matters of foreign intelligence interest; and

d. obtaining information to inform or facilitate intelligence analysis and planning as described in Part IV of these Guidelines.

4. Authorized Methods

Only the following methods may be used in assessments:

a. Obtain publicly available information.
b. Access and examine FBI and other Department of Justice records, and obtain information from any FBI or other Department of Justice personnel.
c. Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies.
d. Use online services and resources (whether nonprofit or commercial).
e. Use and recruit human sources in conformity with the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.
f. Interview or request information from members of the public and private entities.
g. Accept information voluntarily provided by governmental or private entities.
h. Engage in observation or surveillance not requiring a court order.
i. Grand jury subpoenas for telephone or electronic mail subscriber information.

B. PREDICATED INVESTIGATIONS

1. Purposes

Predicated investigations may be carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence.

2. Approval

The initiation of a predicated investigation requires supervisory approval at a level or levels specified by FBI policy. A predicated investigation based on paragraph 3.c. (relating to foreign intelligence) must be approved by a Special Agent in Charge or by an FBI Headquarters official as provided in such policy.

3. Circumstances Warranting Investigation

A predicated investigation may be initiated on the basis of any of the following circumstances:

a. An activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information relating to the

activity or the involvement or role of an individual, group, or organization in such activity.

b. An individual, group, organization, entity, information, property, or activity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity in violation of federal law or a threat to the national security and the investigation may obtain information that would help to protect against such activity or threat.

c. The investigation may obtain foreign intelligence that is responsive to a foreign intelligence requirement.

4. Preliminary and Full Investigations

A predicated investigation relating to a federal crime or threat to the national security may be conducted as a preliminary investigation or a full investigation. A predicated investigation that is based solely on the authority to collect foreign intelligence may be conducted only as a full investigation.

a. Preliminary investigations

i. Predication Required for Preliminary Investigations

A preliminary investigation may be initiated on the basis of information or an allegation indicating the existence of a circumstance described in paragraph 3.a.-.b.

ii. Duration of Preliminary Investigations

A preliminary investigation must be concluded within six months of its initiation, which may be extended by up to six months by the Special Agent in Charge. Extensions of preliminary investigations beyond a year must be approved by FBI Headquarters.

iii. Methods Allowed in Preliminary Investigations

All lawful methods may be used in a preliminary investigation except for methods within the scope of Part V.A. 1 1 .--.13. of these Guidelines.

b. Full Investigations

i. Predication Required for Full Investigations

A full investigation may be initiated if there is an articulable factual basis for the investigation that reasonably indicates that a circumstance described in paragraph 3 .a.-.b. exists or if a circumstance described in paragraph 3 .c. exists.

ii. Methods Allowed in Full Investigations

All lawful methods may be used in a full investigation.

5. Notice Requirements

a. An FBI field office shall notify FBI Headquarters and the United States Attorney or other appropriate Department of Justice official of the initiation by the field office of a predicated investigation involving a

sensitive investigative matter. If the investigation is initiated by FBI Headquarters, FBI Headquarters shall notify the United States Attorney or other appropriate Department of Justice official of the initiation of such an investigation. If the investigation concerns a threat to the national security, an official of the National Security Division must be notified. The notice shall identify all sensitive investigative matters involved in the investigation.

b. The FBI shall notify the National Security Division of:
    i. the initiation of any full investigation of a United States person relating to a threat to the national security; and
    ii. the initiation of any full investigation that is based on paragraph 3.c. (relating to foreign intelligence).
c. The notifications under subparagraphs a. and b. shall be made as soon as practicable, but no later than 30 days after the initiation of an investigation.
d. The FBI shall notify the Deputy Attorney General if FBI Headquarters disapproves a field office's initiation of a predicated investigation relating to a threat to the national security on the ground that the predication for the investigation is insufficient.

C. ENTERPRISE INVESTIGATIONS

1. Definition

A full investigation of a group or organization may be initiated as an enterprise investigation if there is an articulable factual basis for the investigation that reasonably indicates that the group or organization may have engaged or may be engaged in, or may have or may be engaged in planning or preparation or provision of support for:

a. a pattern of racketeering activity as defined in 18 U.S.C. 1961 (5);
b. international terrorism or other threat to the national security;
c. domestic terrorism as defined in 18 U.S.C. 2331(5) involving a violation of federal criminal law;
d. furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law; or
e. an offense described in 18 U.S.C. 2332b(g)(5)(B) or 18 U.S.C. 43.

2. Scope

The information sought in an enterprise investigation may include a general examination of the structure, scope, and nature of the group or organization including: its relationship, if any, to a foreign power; the identity and relationship of its members, employees, or other persons who may be acting in furtherance of its objectives; its finances and resources; its geographical dimensions; and its past and future activities and goals.

3. Notice and Reporting Requirements

a. The responsible Department of Justice component for the purpose of notification and reports in enterprise investigations is the National Security Division, except that, for the purpose of notifications and reports in an enterprise investigation relating to a pattern of racketeering activity that does not involve an offense or offenses described in 18 U.S.C. 2332b(g)(5)(B), the responsible Department of Justice component is the Organized Crime and Racketeering Section of the Criminal Division.
b. An FBI field office shall notify FBI Headquarters of the initiation by the field office of an enterprise investigation.
c. The FBI shall notify the National Security Division or the Organized Crime and Racketeering Section of the initiation of an enterprise investigation, whether by a field office or by FBI Headquarters, and the component so notified shall notify the Attorney General and the Deputy Attorney General. The FBI shall also notify any relevant United States Attorney's Office, except that any investigation within the scope of Part V1.D.1.d of these Guidelines (relating to counterintelligence investigations) is to be treated as provided in that provision. Notifications by the FBI under this subparagraph shall be provided as soon as practicable, but no later than 30 days after the initiation of the investigation.
d. The Assistant Attorney General for National Security or the Chief of the Organized Crime and Racketeering Section, as appropriate, may at any time request the FBI to provide a report on the status of an enterprise investigation and the FBI will provide such reports as requested.

III. ASSISTANCE TO OTHER AGENCIES

The FBI is authorized to provide investigative assistance to other federal, state, local, or tribal, or foreign agencies as provided in this Part.

The investigative assistance authorized by this Part is often concerned with the same objectives as those identified in Part II of these Guidelines -investigating federal crimes and threats to the national security, and collecting foreign intelligence. In some cases, however, investigative assistance to other agencies is legally authorized for purposes other than those identified in Part II, such as assistance in certain contexts to state or local agencies in the investigation of crimes under state or local law, see 28 U.S.C. 540, 540A, 540B, and assistance to foreign agencies in the investigation of foreign law violations pursuant to international agreements. Investigative assistance for such legally authorized purposes is permitted under this Part, even if it is not for purposes identified as grounds for investigation under Part II.

The authorities provided by this Part are cumulative to Part II and do not limit the FBI's investigative activities under Part II. For example, Subpart B.2 in this Part authorizes investigative activities by the FBI in certain circumstances to inform decisions by the President concerning the deployment of troops to deal with civil disorders, and Subpart B.3 authorizes investigative activities to facilitate demonstrations and related public health and safety measures. The requirements and limitations in these provisions for conducting investigations for the specified purposes do not limit the FBI's authority under Part II to investigate federal crimes or threats to the national security that occur in the context of or in connection with civil disorders or demonstrations.

A. THE INTELLIGENCE COMMUNITY

The FBI may provide investigative assistance (including operational support) to authorized intelligence activities of other Intelligence Community agencies.

B. FEDERAL AGENCIES GENERALLY

1. In General

The FBI may provide assistance to any federal agency in the investigation of federal crimes or threats to the national security or in the collection of foreign intelligence, and investigative assistance to any federal agency for any other purpose that may be legally authorized, including investigative assistance to the Secret Service in support of its protective responsibilities.

2. The President in Relation to Civil Disorders

a. At the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division, the FBI shall collect information relating to actual or threatened civil disorders to assist the President in determining (pursuant to the authority of the President under 10 U.S.C. 331-33) whether use of the armed forces or militia is required and how a decision to commit troops should be implemented. The information sought shall concern such matters as:
    i. The size of the actual or threatened disorder, both in number of people involved or affected and in geographic area.
    ii. The potential for violence.
    iii. The potential for expansion of the disorder in light of community conditions and underlying causes of the disorder.
    iv. The relationship of the actual or threatened disorder to the enforcement of federal law or court orders and the likelihood that state or local authorities will assist in enforcing those laws or orders.
    v. The extent of state or local resources available to handle the disorder.
b. Investigations under this paragraph will be authorized only for a period of 30 days, but the authorization may be renewed for subsequent 30 day periods.
c. Notwithstanding Subpart E.2 of this Part, the methods that may be used in an investigation under this paragraph are those described in subparagraphs a.--.d., subparagraph f. (other than pretext interviews or requests), or subparagraph g. of Part II.A.4 of these Guidelines. The Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division may also authorize the use of other methods described in Part II.A.4.

3. Public Health and Safety Authorities in Relation to Demonstrations

a. At the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division, the FBI shall collect information relating to demonstration activities that are likely to require the federal government to take action to facilitate the activities and provide public health and safety measures with respect to those activities. The information sought in such an investigation shall be that needed to facilitate an adequate federal response to ensure public health and safety and to protect the exercise of First Amendment rights, such as:
    i. The time, place, and type of activities planned.
    ii. The number of persons expected to participate.
    iii. The expected means and routes of travel for participants and expected time of arrival.
    iv. Any plans for lodging or housing of participants in connection with the demonstration.

b. Notwithstanding Subpart E.2 of this Part, the methods that may be used in an investigation under this paragraph are those described in subparagraphs a.-.d., subparagraph f. (other than pretext interviews or requests), or subparagraph g. of Part II.A.4 of these Guidelines. The Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division may also authorize the use of other methods described in Part II.A.4.

C. STATE, LOCAL, OR TRIBAL AGENCIES

The FBI may provide investigative assistance to state, local, or tribal agencies in the investigation of matters that may involve federal crimes or threats to the national security, or for such other purposes as may be legally authorized.

D. FOREIGN AGENCIES

1. At the request of foreign law enforcement, intelligence, or security agencies, the FBI may conduct investigations or provide assistance to investigations by such agencies, consistent with the interests of the United States (including national security interests) and with due consideration of the effect on any United States person. Investigations or assistance under this paragraph must be approved as provided by FBI policy. The FBI shall notify the National Security Division concerning investigation or assistance under this paragraph where: (i) FBI Headquarters approval for the activity is required pursuant to the approval policy adopted by the FBI for purposes of this paragraph, and (ii) the activity relates to a threat to the national security. Notification to the National Security Division shall be made as soon as practicable but no later than 30 days after the approval. Provisions regarding notification to or coordination with the Central Intelligence Agency by the FBI in memoranda of understanding or agreements with the Central Intelligence Agency may also apply to activities under this paragraph.
2. The FBI may not provide assistance to foreign law enforcement, intelligence, or security officers conducting investigations within the United States unless such officers have provided prior notification to the Attorney General as required by 18 U.S.C. 951.
3. The FBI may conduct background inquiries concerning consenting individuals when requested by foreign government agencies.
4. The FBI may provide other material and technical assistance to foreign governments to the extent not otherwise prohibited by law.

E. APPLICABLE STANDARDS AND PROCEDURES

1. Authorized investigative assistance by the FBI to other agencies under this Part includes joint operations and activities with such agencies.
2. All lawful methods may be used in investigative assistance activities under this Part.

3. Where the methods used in investigative assistance activities under this Part go beyond the methods authorized in assessments under Part II.A.4 of these Guidelines, the following apply:
   a. Supervisory approval must be obtained for the activity at a level or levels specified in FBI policy.
   b. Notice must be provided concerning sensitive investigative matters in the manner described in Part II.B.5.
   c. A database or records system must be maintained that permits, with respect to each such activity, the prompt retrieval of the status of the activity (open or closed), the dates of opening and closing, and the basis for the activity. This database or records system may be combined with the database or records system for predicated investigations required by Part VI.A.2.

IV. INTELLIGENCE ANALYSIS AND PLANNING

The FBI is authorized to engage in analysis and planning. The FBI's analytic activities enable the FBI to identify and understand trends, causes, and potential indicia of criminal activity and other threats to the United States that would not be apparent from the investigation of discrete matters alone. By means of intelligence analysis and strategic planning, the FBI can more effectively discover crimes, threats to the national security, and other matters of national intelligence interest and can provide the critical support needed for the effective discharge of its investigative responsibilities and other authorized activities. For example, analysis of threats in the context of special events management, concerning public events or activities that may be targeted for terrorist attack, is an authorized activity under this Part.

In carrying out its intelligence functions under this Part, the FBI is authorized to draw on all lawful sources of information, including but not limited to the results of investigative activities under these Guidelines. Investigative activities under these Guidelines and other legally authorized activities through which the FBI acquires information, data, or intelligence may properly be utilized, structured, and prioritized so as to support and effectuate the FBI's intelligence mission. The remainder of this Part provides further specification concerning activities and functions authorized as part of that mission.

A. STRATEGIC INTELLIGENCE ANALYSIS

The FBI is authorized to develop overviews and analyses of threats to and vulnerabilities of the United States and its interests in areas related to the FBI's responsibilities, including domestic and international criminal threats and activities; domestic and international activities, circumstances, and developments affecting the national security; and matters relevant to the conduct of the United States' foreign affairs. The overviews and analyses prepared under this Subpart may encompass present, emergent, and potential threats and vulnerabilities, their contexts and causes, and identification and analysis of means of responding to them.

B. REPORTS AND ASSESSMENTS GENERALLY

The FBI is authorized to conduct research, analyze information, and prepare reports and assessments concerning matters relevant to authorized FBI activities, such as reports and assessments concerning: types of criminals or criminal activities; organized crime groups; terrorism, espionage, or other threats to the national security; foreign intelligence matters; or the scope and nature of criminal activity in particular geographic areas or sectors of the economy.

C. INTELLIGENCE SYSTEMS

The FBI is authorized to operate intelligence, identification, tracking, and information systems in support of authorized investigative activities, or for such other or additional purposes as may be legally authorized, such as intelligence and tracking systems relating to terrorists, gangs, or organized crime groups.

V. AUTHORIZED METHODS

A. PARTICULAR METHODS

All lawful investigative methods may be used in activities under these Guidelines as authorized by these Guidelines. Authorized methods include, but are not limited to, those identified in the following list. The methods identified in the list are in some instances subject to special restrictions or review or approval requirements as noted:

1. The methods described in Part II.A.4 of these Guidelines.
2. Mail covers.
3. Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g., trash covers).
4. Consensual monitoring of communications, including consensual computer monitoring, subject to legal review by the Chief Division Counsel or the FBI Office of the General Counsel. Where a sensitive monitoring circumstance is involved, the monitoring must be approved by the Criminal Division or, if the investigation concerns a threat to the national security or foreign intelligence, by the National Security Division.
5. Use of closed-circuit television, direction finders, and other monitoring devices, subject to legal review by the Chief Division Counsel or the FBI Office of the General Counsel. (The methods described in this paragraph usually do not require court orders or warrants unless they involve physical trespass or non-consensual monitoring of communications, but legal review is necessary to ensure compliance with all applicable legal requirements.)
6. Polygraph examinations.
7. Undercover operations. In investigations relating to activities in violation of federal criminal law that do not concern threats to the national security or foreign intelligence, undercover operations must be carried out in conformity with the Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations. In investigations that are not subject to the preceding sentence because they concern threats to the national security or foreign intelligence, undercover operations involving religious or political organizations must be reviewed and approved by FBI Headquarters, with participation by the National Security Division in the review process.
8. Compulsory process as authorized by law, including grand jury subpoenas and other subpoenas, National Security Letters (1 5 U.S.C. 168 lu, 168 1v; 18 U.S.C. 2709; 12 U.S.C. 3414(a)(5)(A); 50 U.S.C. 436), and Foreign Intelligence Surveillance Act orders for the production of tangible things (50 U.S.C. 1861-63).

9. Accessing stored wire and electronic communications and transactional records in conformity with chapter 121 of title 18, United States Code (18 U.S.C. 2701- 2712).
10. Use of pen registers and trap and trace devices in conformity with chapter 206 of title 18, United States Code (1 8 U.S.C. 3 121-3 127), or the Foreign Intelligence Surveillance Act (50 U.S.C. 1841 -1 846).
11. Electronic surveillance in conformity with chapter 1 19 of title 18, United States Code (18 U.S.C. 2510-2522), the Foreign Intelligence Surveillance Act, or Executive Order 12333 5 2.5.
12. Physical searches, including mail openings, in conformity with Rule 41 of the Federal Rules of Criminal Procedure, the Foreign Intelligence Surveillance Act, or Executive Order 12333 5 2.5. A classified directive provides additional limitation on certain searches.
13. Acquisition of foreign intelligence information in conformity with title VII of the Foreign Intelligence Surveillance Act.

B. SPECIAL REQUIREMENTS

Beyond the limitations noted in the list above relating to particular investigative methods, the following requirements are to be observed:

1. Contacts with Represented Persons

Contact with represented persons may implicate legal restrictions and affect the admissibility of resulting evidence. Hence, if an individual is known to be represented by counsel in a particular matter, the FBI will follow applicable law and Department procedure concerning contact with represented individuals in the absence of prior notice to counsel. The Special Agent in Charge and the United States Attorney or their designees shall consult periodically on applicable law and Department procedure. Where issues arise concerning the consistency of contacts with represented persons with applicable attorney conduct rules, the United States Attorney's Office should consult with the Professional Responsibility Advisory Office.

2. Use of Classified Investigative Technologies

Inappropriate use of classified investigative technologies may risk the compromise of such technologies. Hence, in an investigation relating to activities in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence, the use of such technologies must be in conformity with the Procedures for the Use of Classified Investigative Technologies in Criminal Cases.

C. OTHERWISE ILLEGAL ACTIVITY

1. Otherwise illegal activity by an FBI agent or employee in an undercover operation relating to activity in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence must be approved in conformity with the Attorney General's Guidelines

on Federal Bureau of Investigation Undercover Operations. Approval of otherwise illegal activity in conformity with those guidelines is sufficient and satisfies any approval requirement that would otherwise apply under these Guidelines.

2. Otherwise illegal activity by a human source must be approved in conformity with the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.
3. Otherwise illegal activity by an FBI agent or employee that is not within the scope of paragraph 1.must be approved by a United States Attorney's Office or a Department of Justice Division, except that a Special Agent in Charge may authorize the following:
   a. otherwise illegal activity that would not be a felony under federal, state, local, or tribal law;
   b. consensual monitoring of communications, even if a crime under state, local, or tribal law;
   c. the controlled purchase, receipt, delivery, or sale of drugs, stolen property, or other contraband;
   d. the payment of bribes;
   e. the making of false representations in concealment of personal identity or the true ownership of a proprietary; and
   f. conducting a money laundering transaction or transactions involving an aggregate amount not exceeding $1 million.

      However, in an investigation relating to a threat to the national security or foreign intelligence collection, a Special Agent in Charge may not authorize an activity that may constitute a violation of export control laws or laws that concern the proliferation of weapons of mass destruction. In such an investigation, a Special Agent in Charge may authorize an activity that may otherwise violate prohibitions of material support to terrorism only in accordance with standards established by the Director of the FBI and agreed to by the Assistant Attorney General for National Security.
4. The following activities may not be authorized:
   a. Acts of violence.
   b. Activities whose authorization is prohibited by law, including unlawful investigative methods, such as illegal electronic surveillance or illegal searches.

      Subparagraph a., however, does not limit the right of FBI agents or employees to engage in any lawful use of force, including the use of force in self-defense or defense of others or otherwise in the lawful discharge of their duties.
5. An agent or employee may engage in otherwise illegal activity that could be authorized under this Subpart without the authorization required by paragraph 3 if necessary to meet an immediate threat to the safety of persons or property or to the national security, or to prevent the compromise of an investigation or the loss of a significant

investigative opportunity. In such a case, prior to engaging in the otherwise illegal activity, every effort should be made by the agent or employee to consult with the Special Agent in Charge, and by the Special Agent in Charge to consult with the United States Attorney's Office or appropriate Department of Justice Division where the authorization of that office or division would be required under paragraph 3., unless the circumstances preclude such consultation. Cases in which otherwise illegal activity occurs pursuant to this paragraph without the authorization required by paragraph 3 shall be reported as soon as possible to the Special Agent in Charge, and by the Special Agent in Charge to FBI Headquarters and to the United States Attorney's Office or appropriate Department of Justice Division.

6. In an investigation relating to a threat to the national security or foreign intelligence collection, the National Security Division is the approving component for otherwise illegal activity for which paragraph 3 requires approval beyond internal FBI approval. However, officials in other components may approve otherwise illegal activity in such investigations as authorized by the Assistant Attorney General for National Security.

VI. RETENTION AND SHARING OF INFORMATION

A. RETENTION OF INFORMATION

1. The FBI shall retain records relating to activities under these Guidelines in accordance with a records retention plan approved by the National Archives and Records Administration.
2. The FBI shall maintain a database or records system that permits, with respect to each predicated investigation, the prompt retrieval of the status of the investigation (open or closed), the dates of opening and closing, and the basis for the investigation.

B. INFORMATION SHARING GENERALLY

1. Permissive Sharing

Consistent with law and with any applicable agreements or understandings with other agencies concerning the dissemination 'of information they have provided, the FBI may disseminate information obtained or produced through activities under these Guidelines:

a. within the FBI and to other components of the Department of Justice;
b. to other federal, state, local, or tribal agencies if related to their responsibilities and, in relation to other Intelligence Community agencies, the determination whether the information is related to the recipient's responsibilities may be left to the recipient;
c. to congressional committees as authorized by the Department of Justice Office of Legislative Affairs;
d. to foreign agencies if the information is related to their responsibilities and the dissemination is consistent with the interests of the United States (including national security interests) and the FBI has considered the effect such dissemination may reasonably be expected to have on any identifiable United States person;
e. if the information is publicly available, does not identify United States persons, or is disseminated with the consent of the person whom it concerns;
f. if the dissemination is necessary to protect the safety or security of persons or property, to protect against or prevent a crime or threat to the national security, or to obtain information for the conduct of an authorized FBI investigation; or
g. if dissemination of the information is otherwise permitted by the Privacy Act (5 U.S.C. 552a).

2. Required Sharing

The FBI shall share and disseminate information as required by statutes, treaties, Executive Orders, Presidential directives, National Security Council directives,

Homeland Security Council directives, and Attorney General-approved policies, memoranda of understanding, or agreements.

C. INFORMATION RELATING TO CRIMINAL MATTERS

1. Coordination with Prosecutors

In an investigation relating to possible criminal activity in violation of federal law, the agent conducting the investigation shall maintain periodic written or oral contact with the appropriate federal prosecutor, as circumstances warrant and as requested by the prosecutor. When, during such an investigation, a matter appears arguably to warrant prosecution, the agent shall present the relevant facts to the appropriate federal prosecutor. Information on investigations that have been closed shall be available on request to a United States Attorney or his or her designee or an appropriate Department of Justice official.

2. Criminal Matters Outside FBI Jurisdiction

When credible information is received by an FBI field office concerning serious criminal activity not within the FBI's investigative jurisdiction, the field office shall promptly transmit the information or refer the complainant to a law enforcement agency having jurisdiction, except where disclosure would jeopardize an ongoing investigation, endanger the safety of an individual, disclose the identity of a human source, interfere with a human source's cooperation, or reveal legally privileged information. If full disclosure is not made for the reasons indicated, then, whenever feasible, the FBI field office shall make at least limited disclosure to a law enforcement agency or agencies having jurisdiction, and full disclosure shall be made as soon as the need for restricting disclosure is no longer present. Where full disclosure is not made to the appropriate law enforcement agencies within 180 days, the FBI field office shall promptly notify FBI Headquarters in writing of the facts and circumstances concerning the criminal activity. The FBI shall make periodic reports to the Deputy Attorney General on such nondisclosures and incomplete disclosures, in a form suitable to protect the identity of human sources.

3. Reporting of Criminal Activity

a. When it appears that an FBI agent or employee has engaged in criminal activity in the course of an investigation under these Guidelines, the FBI shall notify the United States Attorney's Office or an appropriate Department of Justice Division. When it appears that a human source has engaged in criminal activity in the course of an investigation under these Guidelines, the FBI shall proceed as provided in the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources. When information concerning possible criminal activity by any other person appears in the course of an investigation under these Guidelines, the FBI shall initiate an investigation of the criminal activity if warranted, and shall proceed as provided in paragraph 1 or 2.

b. The reporting requirements under this paragraph relating to criminal activity by FBI agents or employees or human sources do not apply to otherwise illegal activity that is authorized in conformity with these Guidelines or other Attorney General guidelines or to minor traffic offenses.

D. INFORMATION RELATING TO NATIONAL SECURITY AND FOREIGN INTELLIGENCE MATTERS

The general principle reflected in current laws and policies is that there is a responsibility to provide information as consistently and fully as possible to agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to the national security, except as limited by specific constraints on such sharing. The FBI's responsibilities in this area include carrying out the requirements of the Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (March 4,2003), or any successor memorandum of understanding or agreement. Specific requirements also exist for internal coordination and consultation with other Department of Justice components, and for provision of national security and foreign intelligence information to White House agencies, as provided in the ensuing paragraphs.

1. Department of Justice

a. The National Security Division shall have access to all information obtained by the FBI through activities relating to threats to the national security or foreign intelligence. The Director of the FBI and the Assistant Attorney General for National Security shall consult concerning these activities whenever requested by either of them, and the FBI shall provide such reports and information concerning these activities as the Assistant Attorney General for National Security may request. In addition to any reports or information the Assistant Attorney General for National Security may specially request under this subparagraph, the FBI shall provide annual reports to the National Security Division concerning its foreign intelligence collection program, including information concerning the scope and nature of foreign intelligence collection activities in each FBI field office.
b. The FBI shall keep the National Security Division apprised of all information obtained through activities under these Guidelines that is necessary to the ability of the United States to investigate or protect against threats to the national security, which shall include regular consultations between the FBI and the National Security Division to exchange advice and information relevant to addressing such threats through criminal prosecution or other means.
c. Subject to subparagraphs d. and e., relevant United States Attorneys' Offices shall have access to and shall receive information from the FBI

relating to threats to the national security, and may engage in consultations with the FBI relating to such threats, to the same extent as the National Security Division. The relevant United States Attorneys' Offices shall receive such access and information from the FBI field offices.

d. In a counterintelligence investigation -i.e., an investigation relating to a matter described in Part VII.S.2 of these Guidelines -the FBI's provision of information to and consultation with a United States Attorney's Office are subject to authorization by the National Security Division. In consultation with the Executive Office for United States Attorneys and the FBI, the National Security Division shall establish policies setting forth circumstances in which the FBI will consult with the National Security Division prior to informing relevant United States Attorneys' Offices about such an investigation. The policies established by the National Security Division under this subparagraph shall (among other things) provide that:
    i. the National Security Division will, within 30 days, authorize the FBI to share with the United States Attorneys' Offices information relating to certain espionage investigations, as defined by the policies, unless such information is withheld because of substantial national security considerations; and
    ii. the FBI may consult freely with United States Attorneys' Offices concerning investigations within the scope of this subparagraph during an emergency, so long as the National Security Division is notified of such consultation as soon as practical after the consultation.
e. Information shared with a United States Attorney's Office pursuant to subparagraph c. or d. shall be disclosed only to the United States Attorney or any Assistant United States Attorneys designated by the United States Attorney as points of contact to receive such information. The United States Attorneys and designated Assistant United States Attorneys shall have appropriate security clearances and shall receive training in the handling of classified information and information derived from the Foreign Intelligence Surveillance Act, including training concerning the secure handling and storage of such information and training concerning requirements and limitations relating to the use, retention, and dissemination of such information.
f. The disclosure and sharing of information by the FBI under this paragraph is subject to any limitations required in orders issued by the Foreign Intelligence Surveillance Court, controls imposed by the originators of sensitive material, and restrictions established by the Attorney General or the Deputy Attorney General in particular cases. The disclosure and sharing of information by the FBI under this paragraph that may disclose the identity of human sources is governed by the relevant provisions of the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.

2. White House

In order to carry out their responsibilities, the President, the Vice President, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security Affairs, the National Security Council and its staff, the Homeland Security Council and its staff, and other White House officials and offices require information from all federal agencies, including foreign intelligence, and information relating to international terrorism and other threats to the national security. The FBI accordingly may disseminate to the White House foreign intelligence and national security information obtained through activities under these Guidelines, subject to the following standards and procedures:

a. Requests to the FBI for such information from the White House shall be made through the National Security Council staff or Homeland Security Council staff including, but not limited to, the National Security Council Legal and Intelligence Directorates and Office of Combating Terrorism, or through the President's Intelligence Advisory Board or the Counsel to the President.
b. Compromising information concerning domestic officials or political organizations, or information concerning activities of United States persons intended to affect the political process in the United States, may be disseminated to the White House only with the approval of the Attorney General, based on a determination that such dissemination is needed for foreign intelligence purposes, for the purpose of protecting against international terrorism or other threats to the national security, or for the conduct of foreign affairs. However, such approval is not required for dissemination to the White House of information concerning efforts of foreign intelligence services to penetrate the White House, or concerning contacts by White House personnel with foreign intelligence service personnel.
c. Examples of types of information that are suitable for dissemination to the White House on a routine basis include, but are not limited to:
    i. information concerning international terrorism;
    ii. information concerning activities of foreign intelligence services in the United States;
    iii. information indicative of imminent hostilities involving any foreign power;
    iv. information concerning potential cyber threats to the United States or its allies;
    v. information indicative of policy positions adopted by foreign officials, governments, or powers, or their reactions to United States foreign policy initiatives;
    vi. information relating to possible changes in leadership positions of foreign governments, parties, factions, or powers;
    vii. information concerning foreign economic or foreign political matters that might have national security ramifications; and

viii. information set forth in regularly published national intelligence requirements.

d. Communications by the FBI to the White House that relate to a national security matter and concern a litigation issue for a specific pending case must be made known to the Office of the Attorney General, the Office of the Deputy Attorney General, or the Office of the Associate Attorney General. White House policy may specially limit or prescribe the White House personnel who may request information concerning such issues from the FBI.
e. The limitations on dissemination of information by the FBI to the White House under these Guidelines do not apply to dissemination to the White House of information acquired in the course of an FBI investigation requested by the White House into the background of a potential employee or appointee, or responses to requests from the White House under Executive Order 10450.

3. Special Statutory Requirements

a. Dissemination of information acquired under the Foreign Intelligence Surveillance Act is, to the extent provided in that Act, subject to minimization procedures and other requirements specified in that Act.
b. Information obtained through the use of National Security Letters under 15 U.S.C. 1681v may be disseminated in conformity with the general standards of this Part. Information obtained through the use of National Security Letters under other statutes may be disseminated in conformity with the general standards of this Part, subject to any applicable limitations in their governing statutory provisions: 12 U.S.C. 3414(a)(5)(B); 15 U.S.C. 1681u(f); 18 U.S.C. 2709(d); 50 U.S.C. 436(e).

VII. DEFINITIONS

A. CONSENSUAL MONITORING:

Monitoring of communications for which a court order or warrant is not legally required because of the consent of a party to the communication.

B. EMPLOYEE:

An FBI employee or an employee of another agency working under the direction and control of the FBI.

C. FOR OR ON BEHALF OF A FOREIGN POWER:

The determination that activities are for or on behalf of a foreign power shall be based on consideration of the extent to which the foreign power is involved in:

1. control or policy direction;
2. financial or material support; or
3. leadership, assignments, or discipline.

D. FOREIGN COMPUTER INTRUSION:

The use or attempted use of any cyber-activity or other means, by, for, or on behalf of a foreign power to scan, probe, or gain unauthorized access into one or more U.S.-based computers.

E. FOREIGN INTELLIGENCE:

Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists.

F. FOREIGN INTELLIGENCE REQUIREMENTS:

1. national intelligence requirements issued pursuant to authorization by the Director of National Intelligence, including the National Intelligence Priorities Framework and the National HUMINT Collection Directives, or any successor directives thereto;
2. requests to collect foreign intelligence by the President or by Intelligence Community officials designated by the President; and
3. directions to collect foreign intelligence by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General.

G. FOREIGN POWER:

1. a foreign government or any component thereof, whether or not recognized by the United States;
2. a faction of a foreign nation or nations, not substantially composed of United States persons;

3. an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
4. a group engaged in international terrorism or activities in preparation therefor;
5. a foreign-based political organization, not substantially composed of United States persons; or
6. an entity that is directed or controlled by a foreign government or governments.

H. HUMAN SOURCE:

A Confidential Human Source as defined in the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.

I. INTELLIGENCE ACTIVITIES:

Any activity conducted for intelligence purposes or to affect political or governmental processes by, for, or on behalf of a foreign power.

J. INTERNATIONAL TERRORISM:

Activities that:

1. involve violent acts or acts dangerous to human life that violate federal, state, local, or tribal criminal law or would violate such law if committed within the United States or a state, local, or tribal jurisdiction;
2. appear to be intended:
    i. to intimidate or coerce a civilian population;
    ii. to influence the policy of a government by intimidation or coercion; or
    iii. to affect the conduct of a government by assassination or kidnapping; and
3. occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear to be intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

K. PROPRTETARY:

A sole proprietorship, partnership, corporation, or other business entity operated on a commercial basis, which is owned, controlled, or operated wholly or in part on behalf of the FBI, and whose relationship with the FBI is concealed from third parties.

L. PUBLICLY AVAILABLE:

Information that has been published or broadcast for public consumption, is available on request to the public, is accessible online or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public.

M. RECORDS:

Any records, databases, files, indices, information systems, or other retained information.

N. SENSITIVE INVESTIGATIVE MATTER:

An investigative matter involving the activities of a domestic public official or political candidate (involving corruption or a threat to the national security), religious or political organization or individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other Department of Justice officials.

O. SENSITIVE MONITORING CIRCUMSTANCE:

1. investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years;
2. investigation of the Governor, Lieutenant Governor, or Attorney General of any state or territory, or a judge or justice of the highest court of any state or territory, concerning an offense involving bribery, conflict of interest, or extortion related to the performance of official duties;
3. a party to the communication is in the custody of the Bureau of Prisons or the United States Marshals Service or is being or has been afforded protection in the Witness Security Program; or
4. the Attorney General, the Deputy Attorney General, or an Assistant Attorney General has requested that the FBI obtain prior approval for the use of consensual monitoring in a specific investigation.

P. SPECIAL AGENT IN CHARGE:

The Special Agent in Charge of an FBI field office (including an Acting Special Agent in Charge), except that the functions authorized for Special Agents in Charge by these Guidelines may also be exercised by the Assistant Director in Charge or by any Special Agent in Charge designated by the Assistant Director in Charge in an FBI field office headed by an Assistant Director, and by FBI Headquarters officials designated by the Director of the FBI.

Q. SPECIAL EVENTS MANAGEMENT:

Planning and conduct of public events or activities whose character may make them attractive targets for terrorist attack.

R. STATE, LOCAL, OR TRIBAL:

Any state or territory of the United States or political subdivision thereof, the District of Columbia, or Indian tribe.

S. THREAT TO THE NATIONAL SECURITY:

1. international terrorism;

2. espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons;
3. foreign computer intrusion; and
4. other matters determined by the Attorney General, consistent with Executive Order 12333 or a successor order.

T. UNITED STATES:

When used in a geographic sense, means all areas under the territorial sovereignty of the United States.

U. UNITED STATES PERSON:

Any of the following, but not including any association or corporation that is a foreign power as defined in Subpart G.1.-.3.:

1. an individual who is a United States citizen or an alien lawfully admitted for permanent residence;
2. an unincorporated association substantially composed of individuals who are United States persons; or
3. a corporation incorporated in the United States.

In applying paragraph 2., if a group or organization in the United States that is affiliated with a foreign-based international organization operates directly under the control of the international organization and has no independent program or activities in the United States, the membership of the entire international organization shall be considered in determining whether it is substantially composed of United States persons. If, however, the U.S.-based group or organization has programs or activities separate from, or in addition to, those directed by the international organization, only its membership in the United States shall be considered in determining whether it is substantially composed of United States persons. A classified directive provides further guidance concerning the determination of United States person status.

V. USE:

When used with respect to human sources, means obtaining information from, tasking, or otherwise operating such sources.

Date: 9/29/08

Michael B. Mukasey
Attorney General

III. COURT RULES

Court Rules Relevant to U.S. Intelligence Law

Foreign Intelligence Surveillance Court Rules

As Amended Through June 1, 2010

Court Rules of the Foreign Intelligence Surveillance Court, *available at* http://www.intelligencelaw.com/library/admin/html/fisc_rules_2010.html.

Table of Contents

I. Scope, Construction, and Amendment of Rules

Rule 1: Scope of Rules

These rules govern all proceedings in the Foreign Intelligence Surveillance Court (hereafter, "the Court"). Issues not addressed in these rules may be resolved under the Federal Rules of Criminal Procedure or the Federal Rules of Civil Procedure.

Rule 2: Amendment

Any amendment to these rules shall be prescribed and promulgated in accordance with 28 U.S.C. § 2071.

II. National Security Information

Rule 3:

In all matters, the Court and its staff shall comply with the security measures established pursuant to 50 U.S.C. §§ 1803(c) and 1822(e), as well as Executive Order 12958, "Classified National Security Information," as amended by Executive Order 13292 (or its successor). Each member of the Court's staff must possess security clearances at a level commensurate to the individual's responsibilities.

III. Structure of the Court and Authority of Judges

Rule 4: Structure

(a) Composition: In accordance with 50 U.S.C. § 1803(a), the Court consists of those United States District Court Judges appointed by the Chief Justice of the United States.

(b) Presiding Judge: The Presiding Judge is the Judge so designated by the Chief Justice.

Rule 5: Authority of the Judges

(a) Scope of Authority: Each Judge of the Court may exercise the authority vested by the Foreign Intelligence Surveillance Act, as amended, 50 U.S.C. § 1801 et seq. ("the Act"), including the authority to issue an Order approving electronic surveillance or a physical search, and such other authority, consonant with Article III of the Constitution and other statutes and laws of the United States, to the extent not inconsistent with the Act.

(b) Authority to Refer Matters: Except for matters involving a denial of an application for a Court Order, a Judge may refer any matter to another Judge of the Court with that Judge's consent. If a Judge directs the government to supplement an application, that Judge may direct the government to present the next renewal of that application to that Judge. If a matter is presented to a Judge whose tenure on the Court expires while the matter is pending, the Presiding Judge shall reassign the matter.

(c) Publication of Opinions: On request by a Judge, the Presiding Judge, after consulting with other Judges of the Court, may direct that an Opinion be published. Before publication, the Opinion must be reviewed by the Executive Branch and redacted, as necessary, to ensure that properly classified information is appropriately protected pursuant to Executive Order 12958 as amended by Executive Order 13292 (or its successor).

IV. Attorneys Authorized to Appear Before the Court

Rule 6: License and Other Requirements for Attorneys

An attorney may appear on a matter with the permission of the Judge before whom the matter is pending. An attorney who appears before the Court must be a licensed attorney and a member, in good standing, of the bar of a federal court, except that an attorney who is employed by and represents the United States or any of its agencies in a matter before the Court may appear before the Court regardless of federal bar membership. All attorneys appearing before the Court must have the appropriate security clearances.

V. Clerk's Office

Rule 7: Duties of the Clerk

(a) Duties: The Clerk will support the work of the Court consistent with the directives of the Presiding Judge. The Presiding Judge may permit the duties of the Clerk to be delegated.

(b) Court Records.

(i) Maintenance of Court Records. The Clerk will: (A) maintain the Court's docket and records--including records and recordings of proceedings before the Court--and the seal; (B) accept all documents for filing; (C) keep all records, pleadings, and files in a secure location, making those materials available only to persons authorized to have access to them; and (D) perform any other duties, consistent with the usual powers of a Clerk of Court, as the Presiding Judge may authorize.

(ii) Release of Court Records. Except when Orders or Opinions are provided to the government when issued, no Court records or other materials may be released without prior motion to and Order by the Court. Court records shall be released in conformance with the security measures referenced in Rule 3.

(c) Electronic Filing: The Clerk, when authorized by the Court, may accept and file applications, Orders, and other filings by any reliable, and appropriately secure, electronic means.

VI. Form and Filing of Applications for Court Orders

Rule 8: Form of Applications for Court Order

(a) Compliance With the Foreign Intelligence Surveillance Act: A Federal officer may file an application for a Court Order in accordance with the Foreign Intelligence Surveillance Act. The application must be approved and certified in accordance with the Act. The application must contain the statements and other information required by the Act.

(b) Citations: Each application must contain citations to pertinent provisions of the Act.

(c) Facsimile or Digital Signatures: With the Judge's consent, an application may be submitted by any reliable, and appropriately secure, electronic means, including facsimile.

Rule 9: Time of Submission; Applications

(a) Time of Submission: Other than for an application being submitted following the Attorney General's authorization of emergency physical search, electronic surveillance, or pen register/trap and trace surveillance, proposed applications and orders must be submitted at least seven calendar days before the date of the scheduled hearing. The final application with the Federal officer's written oath or affirmation, and the approval and certification required by the Act, may be submitted later, but no later than two hours before the scheduled hearing.

(b) Notice of Changes: The government may submit an amended application, but it must identify any differences from previous submissions at the time the Court reviews the final application.

Rule 10: New Matters; Supplementation

(a) Notice to the Court: If an application or other request for action involves an issue not previously before the Court--including, but not limited to, novel issues of technology or law--the applicant must inform the Judge of the nature and significance of that issue.

(i) Memorandum Relating to New Technology. Prior to requesting authorization to use a new surveillance or search technique, the government must submit a memorandum to the Court which: (A) explains the technique; (B) describes the circumstances of the likely use of the technique; (C) discusses legal issues apparently raised by the technique; and (D) describes proposed minimization procedures to be applied to the use of the technique. At the latest, the memorandum must be submitted as part of the first application that seeks to employ the new technique.

(ii) Legal Memorandum. If an application or other request for action raises an issue of law not previously considered by the Court, the government must submit a memorandum of law in support of its position on each new issue. At the latest, the memorandum must be submitted as part of the first application that raises the issue.

(b) Correction of Material Facts: If the government discovers that a submission to the Court contained a misstatement or omission of material fact, the government, in writing, must immediately inform the Judge to whom the submission was made of: (i) the misstatement or omission; (ii) any necessary correction; (iii) the

facts and circumstances relevant to the misstatement or omission; (iv) any modifications the government has made or proposes to make in how it will implement any authority granted by the Court; and (v) how the government proposes to dispose of or treat any information obtained as a result of the misstatement or omission.

(c) Disclosure of Non-Compliance: If the government discovers that any authority granted by the Court has been implemented in a manner that did not comply with the Court's authorization, the government, in writing, must immediately inform the Judge to whom the submission was made of: (i) the non-compliance; (ii) the facts and circumstances relevant to the non-compliance; (iii) any modifications the government has made or proposes to make in how it will implement any authority granted by the Court; and (iv) how the government proposes to dispose of or treat any information obtained as a result of the non-compliance.

(d) Supplementation: The Court may require the applicant to furnish any information the reviewing Judge deems necessary for an informed review of that application and any proposed Orders relating to it.

Rule 11: Motions

Unless the Judge who issued the Order granting an application directs otherwise, a motion to amend the Order need not be presented to the Judge who issued it. The Judge to whom a motion is presented may refer the motion for review and determination to the Judge who ruled on the application.

Rule 12: Applications Following Approval of Emergency Authorizations

(a) Notification: A Judge who has been notified of the emergency authorization of electronic surveillance, physical search, or pen register/trap and trace surveillance pursuant to 50 U.S.C. § 1805(f), § 1824(e), or § 1843, may refer the consequent application to another Judge of the Court.

(b) Hearings: To the extent practicable, hearings on applications consequent to emergency authorizations shall be added to regularly scheduled court sessions.

VII. Hearings

Rule 13: Hearings

(a) Scheduling: The Judge to whom an application is presented shall set the time for the hearing.

(b) Ex Parte: Except as provided for under Rule 15, all hearings shall be ex parte and conducted in a secure location and manner.

(c) Appearances: Unless excused, the official supplying the factual information upon which an Order is sought and an attorney for the applicant must attend the hearing, along with other representatives of the government as the Court may direct or permit.

(d) Testimony; Oath; Recording of Proceedings: The Judge may take testimony under oath and receive other evidence. The testimony may be recorded electronically or as the Judge may otherwise direct, consistent with the security measures referenced in Rule 3.

VIII. Orders

Rule 14: Contents

(a) Citations: All Orders must contain citations to pertinent provisions of the Foreign Intelligence Surveillance Act.

(b) Denying Applications.

(i) Written Statement of Reasons. If a Judge denies an application, the Judge must immediately prepare and file a written statement of each reason for the decision and cause a copy of the statement to be served on the government.

(ii) Submission of Previously Denied Applications. When a Judge denies an application, further submission of the application may be made only to that Judge.

(c) Approving Applications; Expiration Date: The expiration date and time of an Order approving an application must be computed on the basis of calendar days, not judicial business days, and must be stated as Eastern Time. Expiration dates must be computed from the date and time of the Court's issuance of an Order, or, if applicable, of the Attorney General's exercise of emergency authorization pursuant to 50 U.S.C. § 1805(f), § 1824(e), or § 1843.

(d) Electronic Signatures: The Judge may sign the Order by any reliable, and appropriately secure, electronic means, including facsimile.

Rule 15: Enforcement; Sanctions

(a) Show Cause Motions: If a person or entity served with a Court Order (the "recipient") fails to comply with that Order, the government may move the Court for an Order to show cause why the recipient should not be held in contempt and sanctioned accordingly. The motion must be filed with the Clerk of the Court and referred to the Judge of the Court who entered the underlying Order.

(b) Proceedings.

(i) An Order to show cause must confirm issuance of the underlying Order, schedule further proceedings, and afford the recipient an opportunity to show cause why the recipient should not be held in contempt.

(ii) Proceedings on motions and Orders to show cause must be in camera. All records of such proceedings must be maintained in conformance with 50 U.S.C. § 1803(c).

(iii) If the recipient fails to show cause for noncompliance with the underlying Order, the Court may find the recipient in contempt and enter any further Orders it deems necessary and appropriate to compel compliance and to sanction the recipient for noncompliance with the underlying Order.

(iv) If the recipient shows cause for noncompliance or if the Court concludes that the underlying Order should not be enforced as issued, the Court may enter any further Orders it deems appropriate.

Rule 16: Returns; Time for Filing; Contents

(a) Time for Filing.

(i) Search Orders. Unless otherwise ordered by the Court, a return must be made following the issuance of a Search Order either at the time of submission of a renewal application or within ninety days of the execution of a Search Order, whichever is sooner.

(ii) Other Orders. The Court may order the filing of other returns at a time and in a manner as it deems appropriate.

(b) Contents: The return must: (i) notify the Court of the execution of the Order; (ii) describe the circumstances and results of the search or other activity including, where appropriate, an inventory; (iii) certify either that the execution was in conformity with the Order, or, if not in conformity, describe any deviation in execution from the Order and explain the reasons for any deviation; and (iv) include any other information as the Court may direct.

IX. Sequestration or Destruction

Rule 17: Sequestration or Destruction

If the government submits material for sequestration, the Presiding Judge may order the government to file a memorandum stating the circumstances of the material's acquisition, reasons for the request to sequester rather than destroy the material, and any other information as the Presiding Judge may direct. The Presiding Judge may direct the Clerk to keep the material, specifying the terms and conditions of its retention, or order the Clerk or the government to destroy the material.

X. Appeals

Rule 18: Motion to Transmit Record

The government may file an appeal within 60 days of the denial of an application. Upon filing the appeal, the government must file a motion to transmit the record to the Foreign Intelligence Surveillance Court of Review (hereafter, "Court of Review").

Rule 19: Transmission of the Record

The Court must transmit the record under seal to the Court of Review as expeditiously as possible, and no later than 30 days after the government's motion. A copy of the Judge's statement of reasons denying the application must be included as part of the record on appeal.

Rule 20: Oral Notification to the Court of Review

The Clerk must orally notify the Presiding Judge of the Court of Review immediately upon receipt of a motion from the government to transmit a record to the Court of Review.

Appendix to the FISA Court Rules: Procedures for Review of Petitions Filed Pursuant to Section 501(F) of the Foreign Intelligence Surveillance Court Act of 1978

As Amended Through June 1, 2010

Appendix to the Court Rules of the Foreign Intelligence Surveillance Court, *available at* http://www.intelligencelaw.com/library/admin/html/fisc_rules_2010.html.

Table of Contents

I: IN GENERAL

§ 1: Limited Scope

These procedures govern the filing and disposition of petitions pursuant to Section 501(f) of the Foreign Intelligence Surveillance Act of 1978, as amended (hereafter, "the Act").

§ 2: Rules of the Foreign Intelligence Surveillance Court Apply

These procedures supplement the Rules of Procedure of the Foreign Intelligence Surveillance Court (available at www.uscourts.gov/rules), which govern all matters before this Court.

II: PETITION AND OTHER PAPERS

§ 3: Filing

(a) Who May File: The recipient of an Order to produce a tangible thing under Section 501 of the Act may file a petition challenging the Order pursuant to Section 501(f) of the Act. A petition may be filed through counsel.

(i) Petitioner's Initial Filing. The petition or other paper initially filed shall include the petitioner's full name, mailing address, email address, and telephone number. If the petitioner is represented by counsel, the petition or other paper initially filed shall include the petitioner's full name and the full name of the petitioner's attorney, as well as the attorney's address, telephone number, email address, facsimile number, and bar membership information.

(ii) Government's Initial Filing. The government's initial response shall include the full name of the attorneys representing the United States, and their mailing addresses, email addresses, telephone numbers, and facsimile numbers.

(b) Where to File.

(i) Challenging an Unclassified Order. Filing a petition and any related papers challenging an unclassified Production Order or Nondisclosure Order may be accomplished by hand delivery or by overnight delivery to the Foreign Intelligence Surveillance Court's Security Officer (hereafter, "the Court Security Officer"), c/o Security and Emergency Planning Staff, United States Department of Justice, Room 6217, 950 Pennsylvania Ave., NW, Washington, DC 20530. A signed original and one copy of all papers must be submitted.

(ii) Challenging a Classified Order. Filing a petition and any related papers challenging a classified Production Order or Nondisclosure Order (i.e., marked Confidential, Secret, or Top Secret), may be accomplished by contacting the Court Security Officer by telephone to receive instructions about how to file and serve the petition and any related papers. (The Court Security Officer may be contacted by calling the Department of Justice Command Center at 202-514-5000, and asking to be directed to the Director, Security and Emergency Planning Staff).

(c) Time to File Petition.

(i) Challenging a Production Order. A petition challenging an Order to produce a tangible thing must be filed within 20 days after the Order has been served.

(ii) Challenging a Nondisclosure Order. A petition challenging a Nondisclosure Order issued under Section 501(d) may not be filed with this Court earlier than one year after the date of the issuance of the Production Order containing the challenged Nondisclosure Order.

(iii) Subsequent Petition Challenging a Nondisclosure Order. If a Judge denies a petition to modify or set aside a Nondisclosure Order, the petitioner may not file with this Court a subsequent petition challenging the same Nondisclosure Order earlier than one year after the date of the denial.

(d) Effective Date of Filing.

(i) By Petitioner. A petition or other papers submitted by the petitioner shall be considered to be filed on the date received by the Court Security Officer. The Court Security Officer shall transmit all submissions to the Clerk of the Foreign Intelligence Surveillance Court (hereafter, "the Clerk of the Court") on the same date that they are received.

(ii) By Government. The government's response and other papers submitted by the government shall be considered to be filed on the date that they are received by the Clerk of the Court.

§ 4: Content of Petition

(a) Grounds for Petition: A petition shall concisely state the factual and legal grounds for modifying or setting aside the challenged Order.

(b) Access to Classified Information: A petition shall state whether the petitioner and/or the petitioner's attorney previously have been provided access to classified information and the circumstances of such access.

(c) Request to Stay Production.

(i) Petition Does Not Automatically Effect a Stay. A petition does not automatically effect a stay of the underlying Order. In order to stay a Production Order, petitioner must request such relief and it must be granted by the judge to whom the matter is assigned.

(ii) Stay May Be Requested Prior to Filing of a Petition. A petitioner may request a stay of a Production Order prior to filing a petition challenging such Order.

(d) Underlying Order: A petition shall include a copy of the Production Order to which it relates and state the date on which such Order was served upon petitioner.

(e) Petitioner's Request for Hearing: A petition shall state whether a hearing is requested and, if so, whether the petitioner (or petitioner's counsel) seeks to appear personally in the Washington, D.C., area at petitioner's expense, or to participate in a hearing via teleconference.

§ 5: Form and Length of Petition and Other Papers

(a) Form: A petition and other papers filed shall be:

(i) on 8 1/2 by 11 inch opaque white paper;

(ii) typed (double space) or reproduced in a manner that produces a clear black image;

(iii) conspicuously marked "SECTION 501(f) PETITION" on the document itself and any accompanying envelope; and

(iv) filed under seal.

(b) Length.

(i) Petition. Unless otherwise authorized by the assigned Judge, a petition shall not exceed 20 pages in length, including any attachment.

(ii) Other Papers.

(A) Government's Response. Unless otherwise authorized by the assigned Judge, the government's response shall not exceed 20 pages in length, including any attachment.

(B) Petitioner's Reply. Unless otherwise authorized by the assigned Judge, the petitioner's reply, if any, shall not exceed 10 pages in length, including any attachment.

(C) Additional Papers. No sur-replies may be filed without leave of the Court.

§ 6: Service

(a) By Petitioner: A petitioner shall, at or before the time of filing a petition or other paper, serve a copy by hand delivery or by overnight delivery on the United States Department of Justice, National Security Division, 950 Pennsylvania Ave., NW, Room 6150, Washington, D.C. 20530 and on the Federal Bureau of Investigation, Office of General Counsel, National Security Law Branch, 935 Pennsylvania Ave., NW, Room 7947, Washington, D.C. 20535.

(b) By Government: The government shall, at or before the time of filing a response or other paper, serve a copy by hand delivery or by overnight delivery on petitioner's counsel of record or, if the petitioner is proceeding pro se, on the petitioner.

§ 7: Computation of Time

In proceedings governed by these procedures, any period of time shall be computed in the manner specified in Rule 6(a) of the Federal Rules of Civil Procedure. The provisions of Rule 6(e) of the Federal Rules of Civil Procedure shall not apply to the computation of time in these proceedings.

§ 8: Notifying Presiding Judge

Upon receipt, the Clerk of the Court shall notify the Presiding Judge of the Foreign Intelligence Surveillance Court that a petition has been received from the Court Security Officer.

(a) Presiding Judge Unavailable: If the Presiding Judge is not reasonably available when the Clerk of the Court receives a petition, the Clerk of the Court shall notify the local Judge, other than the Presiding Judge, who has the most seniority on the Court. If no local Judge is reasonably available, the Clerk of the Court shall notify the Judge with the most seniority on the Foreign Intelligence Surveillance Court who is reasonably available. The Judge who receives notification shall be the Acting Presiding Judge (hereafter, "the Presiding Judge") for the case.

III: ASSIGNMENT TO A JUDGE

§ 9: Assignment

(a) Presiding Judge: Immediately upon receiving notification from the Clerk of the Court that a petition has been filed, the Presiding Judge shall assign the matter to a Foreign Intelligence Surveillance Court Judge in the petition review pool (hereafter, "the Judge"). The Clerk of the Court shall record the date and time of the assignment.

(b) Transmitting Petition: As soon as possible, and no later than 24 hours after being notified by the Presiding Judge that a petition has been assigned to one of the pool Judges, the Clerk of the Court shall transmit the original or a copy of petition to that Judge.

IV: CONSIDERATION OF PETITION

§ 10: Initial Review

(a) When: The Judge shall conduct an initial review of the petition within 72 hours after being assigned the petition.

(b) Frivolous Petition: If the Judge determines that the petition is frivolous, the Judge shall:

(i) immediately deny the petition and affirm the challenged Order;

(ii) promptly provide a written statement of the reasons for the denial; and

(iii) provide a written ruling, together with the statement of reasons, to the Clerk of the Court, who will transmit them to the Court Security Officer for immediate delivery to the petitioner and the government.

(c) Non-Frivolous Petition.

(i) Scheduling. If the Judge determines that the petition is not frivolous, the Judge shall promptly issue an Order that sets a schedule for its consideration. The Clerk of the Court shall transmit a copy of the Order to the petitioner and the government.

(ii) Manner of Proceeding. At the Judge's discretion, a hearing may be held or the proceedings may be conducted solely on the papers submitted by the petitioner and the government.

§ 11: Response and Reply

(a) Government's Response: Unless otherwise ordered by the Judge, the government's response must be filed within 20 days after the issuance of the initial scheduling order. If the government's response, or any other paper the government is permitted to file, contains classified information that is submitted ex parte, the government also shall file with the Court and serve on the petitioner

an unclassified or redacted version. The unclassified or redacted version, at a minimum, should clearly articulate the government's legal arguments.

(b) Petitioner's Reply: The petitioner may file a reply to the government's response within 10 days after the date the government's response is served.

§ 12: Hearing

(a) Request: The petitioner or the government may request a hearing.

(b) Location: Hearings shall be held in the Washington D.C. area at a location to be determined by the Judge.

(c) In Camera: All hearings shall be in camera.

(d) Recording: All hearings shall be recorded, either by sound or stenographic means.

§ 13: Ex Parte Proceedings

At the request of the government, the Judge shall review ex parte and in camera any papers submitted by the government, or portions thereof, which may include classified information.

§ 14: Rulings on Non-frivolous Petitions

(a) Written Statement of Reasons: The Judge shall promptly provide a written statement of the reasons for modifying, setting aside, or affirming a Production or Nondisclosure Order. The statement may include classified information.

(b) Reinstatement of Underlying Order: If the Judge does not modify or set aside the underlying Order, the Judge shall immediately affirm it and order the recipient to comply therewith.

(c) Transmitting the Judge's Ruling: The Clerk of the Court shall transmit the Judge's ruling and written statement of reasons to the Court Security Officer for immediate delivery to the petitioner and the government. If the Judge's ruling or written statement contains classified information, an unclassified or redacted version shall be provided to the petitioner.

§ 15: Appeals and Sanctions

(a) Appeals: The government or the petitioner may request the Foreign Intelligence Surveillance Court of Review to review the Judge's ruling.

(b) Failure to Comply: If a recipient fails to comply with an Order affirmed under Section 501(f) of the Act and these procedures, the government, pursuant to Rule 15 of the Foreign Intelligence Surveillance Court Rules of Procedure, may file a motion with the Foreign Intelligence Surveillance Court (for referral to the Judge of the Court who entered the underlying Order) seeking enforcement of the affirmed Order. The Court may consider the government's motion without convening further proceedings on the matter.

Alien Terrorist Removal Court Rules

As Amended Through June 1, 2010

Rules of the Alien Terrorist Removal Court of the United States (Effective May 28, 1997), *available at* http://www.intelligencelaw.com/library/admin/html/atrc_rules_2010.html.

Rule 1: Name of Court

This Court, established pursuant to the Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, Title IV, 110 Stat. 1214, 1258, (Title V of the Immigration and Nationality Act), and as amended by the Omnibus Consolidated Appropriations Act for 1997, Public Law No. 104-208, Title I, § 354, 110 Stat. 3009, shall be known as the Alien Terrorist Removal Court of the United States (8 U.S.C. § 1531 et seq.).

Rule 2: Seal

The seal of the Court shall contain the words "Alien Terrorist Removal Court" in the upper sector of space included within the two outer concentric circles and the words "of the United States of America" in the lower sector, and shall contain the standardized eagle rampant in the center.

Rule 3: Situs

The situs of the Court shall be at the United States Courthouse, Washington, D.C., 20001.

Rule 4: Clerk

(a) The Clerk of the District Court for the District of Columbia shall be the Clerk of this Court.

(b) The Clerk shall supply a deputy clerk and other personnel as the business of this Court may require.

(c) Personnel responsible for filing and maintaining records of this Court containing classified information shall have appropriate levels of security clearance in compliance with Executive Branch procedures governing classified information.

Rule 5: Application for Removal

(a) The Attorney General, acting on behalf of the United States as applicant, shall file an original and two copies of an application seeking removal of an alleged alien, named as respondent.

(b) The application shall be submitted ex parte and in camera and shall be filed under seal with the Clerk of this Court.

(c) The application shall state, to the extent known, the level of classified information, if any, that the Attorney General will present in support of removal.

(d) The application shall state whether the respondent is a permanent resident alien.

Rule 6: Assignment of Cases

(a) The Clerk shall promptly advise the Chief Judge, by a secured means, of the filing of an application. The Chief Judge shall thereupon make an assignment of the case to a member of the Court for consideration and determination of that case.

(b) Cases shall be assigned to judges of the Court in such a manner that each judge, if available for an assignment, shall receive an assignment before any other judge receives a second or successive assignment.

Rule 7: Service of an Order Granting an Application and Notice of a Removal Hearing

(a) If an order is entered granting an ex parte application, an authorized representative of the Attorney General shall serve the respondent who is the subject of the application with a copy of the order, excluding any classified information in the order, together with a Notice pursuant to 8 U.S.C. § 1534(b). The Notice shall also set an expeditious date for the Removal Hearing.

(b) The Attorney General shall file with the Clerk a certificate of service of the order and Notice.

(c) Retained counsel for a respondent shall promptly file an appearance with the Clerk.

(d) If a respondent is financially unable to obtain adequate representation, the respondent may request appointment of counsel from the Criminal Justice Panel for United States District Court for the District of Columbia, as provided for in Section 3006A of Title 18 (Criminal Justice Act).

Rule 8: Interim Hearing

(a) For the convenience of the assigned judge and the parties, the judge may conduct an Interim Hearing or Hearings for the purpose of resolving issues relating to representation of the respondent, special issues relating to a permanent resident alien respondent, issues relating to classified information, or if required by statute. When appropriate, the Interim Hearing will be conducted ex parte and in camera.

(b) Any Interim Hearing shall be conducted in the United States Courthouse in Washington, D.C.

Rule 9: Place of Conducting Removal Hearing

The Removal Hearing shall be held in the United States Courthouse in Washington, D.C. The Removal Hearing shall be conducted publicly, except that any part of the argument that refers to evidence received in camera and ex parte, shall be heard in camera and ex parte.

Rule 10: Verbatim Record of Proceedings

All ex parte, in camera, and public hearings of the Court shall be recorded verbatim by a reporter retained pursuant to 28 U.S.C. § 753, by shorthand, mechanical means, electronic sound recording, or any other method, subject to regulations promulgated by the Judicial Conference of the United States.

Rule 11: Motions

(a) Any motion shall include or be accompanied by a statement of the specific points of law and authority that support the motion, including where appropriate a concise statement of facts. If a table of cases is provided, counsel shall place asterisks in the margin to the left of those cases or authorities on which counsel chiefly relies.

(b) Within 15 days of the date of service or at such other time as the assigned judge may direct, an opposing party shall serve and file a memorandum of points and authorities in opposition to the motion. If such a memorandum is not filed within the prescribed time, the judge may treat the motion as uncontested.

(c) Each motion shall be accompanied by a proposed order.

(d) Within 10 days after service of the memorandum in opposition, the moving party may serve and file a reply memorandum.

(e) A memorandum of points and authorities in support of or in opposition to a motion shall not exceed 15 pages and a reply memorandum shall not exceed 10 pages, without prior approval of the assigned judge.

(f) A party may in a motion or opposition request oral argument, but its allowance shall be within the discretion of the assigned judge.

Rule 12: Subpoenas

Except for good cause shown, requests for issuance of a subpoena pursuant to 8 U.S.C. § 1534(d) by either the respondent or applicant, shall be made at least 10 days prior to the date of the removal hearing.

Rule 13: Classified Information

(a) The ex parte and in camera examination of any classified information, pursuant to 8 U.S.C. § 1534(e)(3)(A)-(E), and of the proposed unclassified summary of specific information shall both be conducted on the day of the Interim Hearing unless the assigned judge otherwise directs.

(b) The unclassified summary, following approval by the judge, shall be delivered to the respondent without delay.

(c) When the respondent is a lawful permanent resident alien, who is denied an unclassified summary pursuant to 8 U.S.C. § 1534(e)(3)(F), the judge shall designate a special attorney to assist the respondent by reviewing the classified information.

(d) When the appointed special attorney moves to challenge the veracity of the evidence contained in the classified information pursuant to 8 U.S.C. § 1534(e)(3)(F)(i)(II), the assigned judge shall schedule an in camera proceeding prior to the Removal Hearing to consider the motion.

Rule 14: Removal Hearing Memorandum

Seven days prior to the Removal Hearing, counsel for the applicant and the respondent shall file with the Clerk and serve on each other a Hearing Memorandum setting forth any legal issues to be raised, a summary of the anticipated testimony (exclusive of classified information), and copies of exhibits (exclusive of classified information). The names of individuals involved in the investigation and prospective witnesses need not be included in the material filed with the Court.