

**APPENDIX 9
INTELLIGENCE LAW**

Appendix 9-1: DoDD 5143.01 – Undersecretary of Defense for Intelligence

See next page.



Department of Defense

DIRECTIVE

NUMBER 5143.01

November 23, 2005

DA&M

SUBJECT: Under Secretary of Defense for Intelligence (USD(I))

- References:
- (a) Title 10, United States Code
 - (b) Title 50, United States Code
 - (c) Public Law 108-458, "Intelligence Reform and Terrorism Prevention Act of 2004," 118 Stat. 3638, December 17, 2004
 - (d) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
 - (e) through (ad), see enclosure 1

1. PURPOSE

Under the authorities vested in the Secretary of Defense by reference (a), including Sections 113 and 137, and consistent with reference (b), including Sections 401 through 405, as well as references (c), (d), and Executive Order (E.O.) 13355 (reference (e)), this Directive:

- 1.1. Assigns the responsibilities, functions, relationships, and authorities of the Under Secretary of Defense for Intelligence (USD(I)).
- 1.2. Cancels the Secretary of Defense Memorandum, "Office of the Under Secretary of Defense for Intelligence"; the Deputy Secretary of Defense Memorandum, "Implementation Guidance on Restructuring Defense Intelligence—and Related Matters"; and DoD Directive 5134.11 (references (f) through (h)).
- 1.3. Authorizes the USD(I), as a Principal Staff Assistant (PSA) reporting directly to the Secretary of Defense, to promulgate DoD policy in DoD Instructions within the responsibilities, functions, and authorities assigned herein.
- 1.4. Shall conform to and be consistent with law and Presidential guidance concerning the authorities and responsibilities of the Director of National Intelligence (DNI).

DoDD 5143.01, November 23, 2005

2. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense, the Military Departments, 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”).

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. RESPONSIBILITIES AND FUNCTIONS

The USD(I) is the PSA and advisor to the Secretary and Deputy Secretary of Defense regarding intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters (hereafter referred to as “intelligence, counterintelligence, and security” matters). In this capacity, the USD(I) exercises the Secretary of Defense’s authority, direction, and control over the Defense Agencies and DoD Field Activities that are Defense intelligence, counterintelligence, or security Components and exercises planning, policy, and strategic oversight over all DoD intelligence, counterintelligence, and security policy, plans, and programs. In the exercise of assigned responsibilities, the USD(I) shall:

4.1. Serve as the senior DoD intelligence, counterintelligence, and security official below the Secretary and Deputy Secretary of Defense.

4.2. Serve as the primary representative of the Secretary of Defense to the Office of the Director of National Intelligence (ODNI) and other members of the Intelligence Community.

4.3. For human capital:

4.3.1. Consistent with DoD Directive 1400.35 (reference (i)), exercise policy oversight of personnel in defense intelligence positions to ensure that Defense intelligence, counterintelligence, and security Components are manned, trained, equipped, and structured to support the missions of the Department and fully satisfy the needs of the Combatant Commands, the Military Departments, and the ODNI, as appropriate.

4.3.2. Develop and oversee the policies associated with the Defense Civilian Intelligence Personnel System in conjunction with the Under Secretary of Defense for Personnel and Readiness pursuant to reference (i).

DoDD 5143.01, November 23, 2005

4.3.3. Develop policy and provide oversight on training, education, and career development of personnel within the Defense intelligence, counterintelligence, and security Components and ensure integration of Defense intelligence into other DoD training within the Department of Defense and Intelligence Community, as appropriate.

4.3.4. Identify candidates for Secretary of Defense consideration to be nominated and/or appointed to serve as Directors of the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and the National Security Agency/Central Security Service.

4.3.5. Oversee the duty performance of the Directors of the Defense Intelligence Components (identified in paragraph 5.1.2) and solicit evaluative input from the DNI, as appropriate.

4.3.6. Oversee the implementation of DoD detailee policy within the Defense intelligence, counterintelligence, and security Components, and exercise approval authority, consistent with the processes developed by the Secretary of Defense and the DNI, over the assignment of intelligence, counterintelligence, and security personnel, including personnel who are subject to the Defense Civilian Intelligence Personnel System, detailed to duty from one DoD Component to another or to an external organization. All requests for detailees external to the Department to perform duties in the fields of intelligence, counterintelligence, or security shall receive the concurrence of the USD(I) prior to approval by the Director of Administration and Management pursuant to applicable law, regulations, and policy, including DoD Directive 1000.17 (reference (j)).

4.4. For planning, programming, budgeting, and execution matters, and other budgetary matters, consistent with Section 135 of 10 U.S.C. (reference (a)):

4.4.1. Participate, pursuant to the responsibilities and functions prescribed herein, in the DoD Planning, Programming, Budgeting, and Execution (PPBE) process, which includes proposing DoD resource programs, formulating budget estimates, recommending resource allocations and priorities, and monitoring the implementation of approved programs in order to ensure adherence to approved policy and planning guidance. The USD(I) shall consult and coordinate with the Under Secretary of Defense for Policy (USD(P)), the Under Secretary of Defense (Comptroller) (USD(C)), and the Director, Program Analysis and Evaluation (DPA&E) on PPBE matters.

4.4.2. Support the Assistant Secretary of Defense for Legislative Affairs and USD(C) in presenting, justifying, and defending intelligence, counterintelligence, and security programs and budgets before the Congress as well as evaluating and assessing Congressional activity for impact on all assigned areas of responsibility, and consult and coordinate with the USD(C) on budgetary matters, as appropriate, and the DNI on National Intelligence Program (NIP) matters.

DoDD 5143.01, November 23, 2005

4.4.3. Oversee Defense intelligence, counterintelligence, and security policy, plans, programs, required capabilities, and resource allocations, which includes exercising responsibility for the DoD Components within the NIP and the Military Intelligence Program (MIP), according to Deputy Secretary of Defense Memorandum (reference (k)).

4.4.4. Oversee all Defense intelligence budgetary matters to ensure compliance with the budget policies issued by the DNI for the NIP.

4.5. For acquisition matters:

4.5.1. Provide advice and assistance, as appropriate, to the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, the Defense Acquisition Board, the Defense Space Acquisition Board, the DNI, and other officials and/or entities in the U.S. Government concerning acquisition programs that significantly affect Defense intelligence, counterintelligence, and security Components as well as intelligence, counterintelligence, and security programs.

4.5.2. Exercise acquisition authority as delegated by the USD(AT&L), the DNI, or other appropriate officials in the U.S. Government for the acquisition of technologies, systems, and equipment.

4.5.3. In coordination with the USD(AT&L), oversee the exercise of acquisition authority by the Directors of the Defense intelligence, counterintelligence, and security Components.

4.6. Provide policy and strategic oversight of all Defense intelligence, counterintelligence, and security programs within the Department of Defense operating under the authority, direction, and control of the USD(I) as prescribed herein, and ensure that these organizations perform their missions.

4.7. Ensure that USD(I) policies and programs are designed and managed to improve standards of performance, economy, and efficiency and that all of the Defense Agencies and DoD Field Activities over which the USD(I) exercises the Secretary of Defense's authority, direction, and control are attentive and responsive to the requirements of their organizational customers, both internal and external to the Department of Defense.

4.8. Serve on boards, committees, and other groups pertaining to assigned responsibilities and functions and represent the Secretary of Defense on all intelligence, counterintelligence, and security matters in other U.S. Government fora.

4.9. For Defense intelligence:

DoDD 5143.01, November 23, 2005

4.9.1. Oversee all DoD intelligence policies and activities, including those implemented pursuant to DoD Directive 5240.1 (reference (l)), and establish priorities to ensure conformance with Secretary of Defense and DNI policy guidance, as appropriate.

4.9.2. Develop, coordinate, and oversee the implementation of DoD policy, strategy, programs, and guidance on manned and unmanned spaceborne, airborne, surface, and subsurface activities and other matters pertaining to intelligence, surveillance, and reconnaissance (ISR), including those in support of foreign and international requirements involving the use of space and non-space resourced ISR activities and products.

4.9.3. Oversee Sensitive Reconnaissance Operations (SRO) Program policy and maintain cognizance of non-SRO reconnaissance and surveillance activities and operations.

4.9.4. Develop and oversee policy for Defense intelligence planning and preparation activities as well as Defense warning and forecasting activities.

4.10. For counterintelligence:

4.10.1. Represent the Secretary of Defense in meetings and communications with the National Counterintelligence Executive (NCIX).

4.10.2. Develop, coordinate, and oversee the implementation of DoD policy, programs, and guidance for DoD counterintelligence pursuant to DoD Directive 5240.2 (reference (m)) and oversee and provide guidance to ensure compliance with counterintelligence policies issued by the DNI, as appropriate.

4.10.3. Oversee DoD polygraph policies and ensure the Department of Defense supports the polygraph requirements identified by the heads of other Federal Agencies with polygraph programs.

4.10.4. Promptly inform the Secretary and Deputy Secretary of Defense, OSD PSAs, Secretaries of the Military Departments, Chairman of the Joint Chiefs of Staff as well as the DNI, NCIX, and Congress of significant counterintelligence activity, as appropriate.

4.11. For security policy matters:

4.11.1. Serve as the DoD Senior Security Official pursuant to E.O. 12958 (reference (n)) and advise the Secretary of Defense, the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, and the Heads of other DoD Components on the development and integration of risk-managed security and protection policies and programs, except for Nuclear Physical Security pursuant to DoD Directive O-5210.41 (reference (o)).

4.11.2. Develop, coordinate, and oversee the implementation of DoD policy, programs, and guidance for personnel, physical, industrial, information, operations, chemical/biological, and DoD Special Access Program (SAP) security as well as research and technology protection.

DoDD 5143.01, November 23, 2005

4.11.2.1. Oversee the implementation of policy regarding the protection of sensitive compartmented information pursuant to Presidential and DNI guidance as well as DoD Directive 8520.1 (reference (p)).

4.11.2.2. Perform all duties and responsibilities of the Secretary of Defense regarding the National Industrial Security Program pursuant to E.O. 12829 (reference (q)).

4.11.3. Develop and oversee DoD policy regarding the sharing of information consistent with applicable laws, regulations, and policy, including E.O. 12333 (reference (d)), DNI policies, and DoD policies.

4.11.3.1. Ensure that all DoD Components integrate security education and awareness into their personnel-security programs pursuant to E.O. 12968 (reference (r)).

4.11.3.2. Develop and oversee DoD SAP security policy, carry out guidance provided by the DoD SAP Oversight Committee, serve as the oversight authority for all DoD Intelligence SAPs and those SAPs delegated to the USD(I) for oversight, and establish a SAP Coordination Office (SAPCO) in OUSD(I) that provides administrative support to and facilitates the management of SAPs delegated to the USD(I), and ensure that all NIP-funded SAPs are consistent with DNI policies and coordinated with the ODNI.

4.12. Serve as the DoD focal point for all policy and oversight matters relating to intelligence information sharing and interoperability of Defense intelligence systems and processes pursuant to reference (c) and E.O. 13356 and E.O. 13354 (references (s) and (t)). The USD(I) shall develop, coordinate, and oversee DoD requirements and compliance with intelligence information sharing and interoperability requirements and policies issued by the DNI.

4.13. For Information Operations (IO):

4.13.1. Serve as the PSA and advise the Secretary of Defense on development and oversight of DoD IO policy and integration activities, and serve as the DoD lead with the Intelligence Community on DoD IO Issues.

4.13.2. Coordinate, oversee, and assess the efforts of the DoD Components to plan, program, and develop capabilities in support of IO requirements pursuant to DoD Directive S-3600.1 (reference (u)).

4.13.3. Provide IO assessments for Operational Plans and Security Cooperation Guidance in support of the USD(P).

4.14. Oversee Defense Sensitive Support Program policy pursuant to DoD Directive S-5210.36 (reference (v)), oversee coordination pursuant to the DNI's policy and guidance, currently DCID 5/1 (reference (w)), and oversee the Defense Cover Program.

DoDD 5143.01, November 23, 2005

4.15. Pursuant to 10 U.S.C. (reference (a)), 50 U.S.C. (reference (b)), and Secretary of Defense guidance, develop policies and implementation guidance, as well as provide oversight to ensure versatility and agility in meeting the Department's missions.

4.16. Develop, coordinate, and oversee policy and policy implementation for all other sensitive intelligence, counterintelligence, security, and special technology programs and activities within the Department of Defense.

4.17. Identify gaps and opportunities for technology insertion to enhance intelligence, counterintelligence, and security capabilities of the Department and, in conjunction with USD(AT&L), Director of Operational Test and Evaluation, Director of Defense Research and Engineering, and other OSD PSAs, as appropriate, oversee research, development, test, and evaluation, subject to DoD acquisition regulations and Sections 139 and 2399 of 10 U.S.C. (reference (a)). NIP-funded programs shall be undertaken in coordination with the DNI.

4.18. Periodically assess any DoD Executive Agent assignments under the cognizance of the USD(I) for continued need, currency, and effectiveness and efficiency in satisfying end user requirements, consistent with DoD Directive 5101.1 (reference (x)).

4.19. Coordinate with the USD(P) regarding intelligence and intelligence-related matters that affect antiterrorism, counterterrorism, and terrorism consequence management policies as well as special operations intelligence elements and special operations-related activities funded through the MIP.

4.20. Perform such other duties as the Secretary may prescribe.

5. RELATIONSHIPS

5.1. The Under Secretary of Defense for Intelligence, in the performance of assigned functions and responsibilities, shall take precedence in the Department of Defense on all intelligence, counterintelligence, and security matters prescribed herein after the Secretary and Deputy Secretary of Defense, and shall:

5.1.1. Report directly to the Secretary of Defense.

5.1.2. Exercise the Secretary of Defense's authority, direction, and control over:

5.1.2.1. Director, Defense Security Service;

5.1.2.2. Director, DoD Counterintelligence Field Activity;

5.1.2.3. Director, Defense Intelligence Agency;

5.1.2.4. Director, National Geospatial-Intelligence Agency;

DoDD 5143.01, November 23, 2005

5.1.2.5. Director, National Security Agency/Central Security Service;

5.1.2.6. Director, National Reconnaissance Office; and

5.1.2.7. Such other positions and organizations as may be established by the USD(I), consistent with applicable law, within the resources provided by the Secretary of Defense.

5.1.3. Exercise the Secretary of Defense's authority, direction, and control over the Directors listed in subparagraphs 5.1.2.3 through 5.1.2.6 above, in consultation with the DNI regarding national intelligence and related matters under the purview of the DNI, as appropriate, consistent with Secretary of Defense and DNI responsibilities under 50 U.S.C. (reference (b)) and the "Intelligence Reform and Terrorism Prevention Act of 2004" (reference (c)).

5.1.4. Serve as the Secretary of Defense's focal point pursuant to responsibilities and functions prescribed herein with other government entities, including the National Security Council, Homeland Security Council, Department of the Treasury, Department of State, Department of Justice, and Department of Homeland Security as well as foreign governments, international organizations, state agencies, the Intelligence Community, and Congress.

5.1.5. As Program Executive for the Military Intelligence Program pursuant to Acting Deputy Secretary of Defense Memorandum (reference (k)), provide policy, guidance, and oversight and establish mechanisms for the appropriate coordination with USD(P), USD(C), DPA&E, and Chairman of the Joint Chiefs of Staff throughout the DoD planning, programming, budgeting, and execution cycles, according to DoD Directive 7045.14 (reference (y)). The USD(I) will work in close concert with the DNI, as appropriate. The USD(I) shall chair or participate in, as appropriate, groups established to address programmatic issues.

5.1.6. Make recommendations to the USD(C) on all transfers, realignments, and/or reprogramming of funds to and from the Military Intelligence Program in accordance with thresholds established in the Financial Management Regulation (reference (z)). The USD(I) shall consult with the ODNI in advance of transferring or reprogramming funds made available under the Military Intelligence Program. In addition, the USD(I) shall coordinate or consult with other OSD PSAs and Heads of the DoD Components, as appropriate, on all reprogramming plans.

5.1.7. For national intelligence centers established by the DNI:

5.1.7.1. Coordinate with the USD(P) as well as the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, and other OSD PSAs, as appropriate, to ensure that DoD support to national intelligence centers is provided, as necessary, and comply with DoD Directive 1000.17 (reference (j)), as applicable.

5.1.7.2. Provide policy, oversight, and guidance for all Defense intelligence, counterintelligence, and security support provided to national intelligence centers, including the National Counterterrorism Center and the National Counterproliferation Center as well as similar activities.

DoDD 5143.01, November 23, 2005

5.1.8. Coordinate with the Inspector General of the Department of Defense and the Assistant to the Secretary of Defense for Intelligence Oversight to ensure that Defense intelligence, counterintelligence, and security Components and DoD activities comply with statutory, Executive, Departmental and other national policies, guidance, and regulations.

5.1.9. Work closely with the USD(P) to ensure that space-based-intelligence systems support the Secretary of Defense and his position regarding national security space policy.

5.1.10. Work closely with the DoD Executive Agent for Space regarding his or her DoD-wide responsibilities representing and advocating space interests in the planning and programming processes and Defense acquisition process, pursuant to the DoD Directive 5101.2 (reference (aa)).

5.1.11. Work closely with the Chairman of the Joint Chiefs of Staff in carrying out functions under Section 153 of reference (a) to ensure the development of intelligence, counterintelligence, and security programs that enhance interoperability and effectively support the joint warfighting responsibilities of the Commanders of the Combatant Commands consistent with Sections 164, 167, and 167a of 10 U.S.C. (reference (a)).

5.1.12. Work closely with the DNI to ensure effective, complementary, and mutual support between Defense intelligence programs and the NIP.

5.1.13. Use existing systems, facilities, and services of the Department of Defense and other Federal Agencies, when practicable, to avoid duplication and to achieve maximum readiness, sustainability, economy, and efficiency.

5.1.14. Coordinate and exchange information with other OSD officials and the Heads of the DoD Components having collateral or related responsibilities and functions.

5.2. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, pursuant to DoD Directive 5144.1 (reference (ab)), shall work closely with the USD(I) on all matters prescribed herein, as appropriate.

5.3. The General Counsel of the Department of Defense shall serve as the legal advisor to the Secretary of Defense, the Deputy Secretary of Defense, the USD(I), and other DoD officials, as appropriate, regarding legal matters associated with intelligence, counterintelligence, and security matters and shall consult as appropriate with the USD(I) on such matters.

5.4. The Heads of the Defense Intelligence Components shall ensure, to the extent possible, USD(I) receipt of intelligence estimates or other substantive and time-sensitive intelligence produced by the Defense Intelligence Components and submitted to the Secretary of Defense, Deputy Secretary of Defense, and the Chairman of the Joint Chiefs of Staff as well as the DNI or other senior officials outside of the Department of Defense.

DoDD 5143.01, November 23, 2005

5.5. The other Office of the Secretary of Defense officials and the Heads of the DoD Components shall coordinate with the USD(I) on all matters related to the authorities, responsibilities, and functions assigned in this Directive.

5.6. The Secretaries of the Military Departments shall provide timely advice to the USD(I) and shall ensure that the policies and guidance issued by the USD(I) are implemented in their respective Military Departments.

5.7. The Chairman of the Joint Chiefs of Staff shall consult with, and seek the advice of, the Combatant Commanders on policy, programs, and other related activities that support the Department's intelligence, counterintelligence, and security goals and missions, including requests for advice, resources, assistance, and other functions pursuant to Section 153 of 10 U.S.C. (reference (a)). The Chairman of the Joint Chiefs of Staff shall facilitate communications with the Combatant Commanders to ensure intelligence, counterintelligence, and security interoperability and support for joint warfighting, particularly as they relate to intelligence-related functions prescribed herein and consistent with Sections 164, 167, and 167a of 10 U.S.C. (reference (a)).

6. AUTHORITIES

The USD(I) is hereby delegated authority to:

6.1. Issue in DoD Instructions, DoD policy within the authorities and responsibilities assigned herein, including authority to identify collateral responsibilities of OSD officials and the Heads of the DoD Components. Such Instructions shall be fully coordinated in accordance with DoD 5025.1-M (reference (ac)). Further, in areas of assigned responsibilities and functions, the USD(I) has authority to issue other DoD Instructions, DoD Publications, and one-time directive-type memoranda, consistent with reference (ac), that implement policy approved by the Secretary of Defense. Instructions to the Military Departments shall be issued through the Secretaries of the Military Departments. Instructions to the Combatant Commands normally shall be communicated through the Chairman of the Joint Chiefs of Staff.

6.2. Obtain reports and information, consistent with DoD Directive 8910.1 (reference (ad)), as necessary in carrying out assigned responsibilities and functions.

6.3. Communicate directly with the Office of the DNI on Defense intelligence matters on behalf of the Secretary of Defense.

6.4. Communicate directly with the Heads of the DoD Components, as necessary, to carry out assigned functions and responsibilities, including the transmission of requests for advice and assistance. Communications to the Military Departments shall be through the Secretaries of the Military Departments, their designees, or as otherwise provided in law or directed by the Secretary of Defense in other DoD issuances. Communications to the Commanders of the Combatant Commands normally shall be transmitted through the Chairman of the Joint Chiefs of Staff.

APPENDIX 9: INTELLIGENCE LAW

DoDD 5143.01, November 23, 2006

6.5. Establish arrangements for DoD participation in U.S. Governmental programs for which the USD(I) is assigned primary DoD cognizance.

6.6. Communicate with other Government officials, representatives of the Legislative Branch, members of the public, and representatives of foreign governments, as appropriate, in carrying out assigned responsibilities and functions.

6.7. Exercise the delegations of authority in enclosure 3.

7. EFFECTIVE DATE

This Directive is effective immediately.

A handwritten signature in black ink, appearing to read "D. Rumsfeld". The signature is written in a cursive, somewhat stylized font.

Enclosures — 3

- E1. References, continued
- E2. Definitions
- E3. Delegations of Authority

DoDD 5143.01, November 23, 2005

E1. ENCLOSURE 1REFERENCES, continued

- (e) Executive Order 13355, "Strengthened Management of the Intelligence Community," August 27, 2004
- (f) Secretary of Defense Memorandum, "Office of the Under Secretary of Defense for Intelligence," April 18, 2003 (hereby canceled)
- (g) Deputy Secretary of Defense Memorandum, "Implementation Guidance on Restructuring Defense Intelligence—and Related Matters," May 8, 2003 (hereby canceled)
- (h) DoD Directive 5134.11, "Defense Airborne Reconnaissance Office (DARO)," April 5, 1995 (hereby canceled)
- (i) DoD Directive 1400.35, "Defense Civilian Intelligence Personnel System (DCIPS)," March 18, 2002
- (j) DoD Directive 1000.17, "Detail of DoD Personnel to Duty Outside the Department of Defense," February 24, 1997
- (k) Acting Deputy Secretary of Defense Memorandum, "Establishment of the Military Intelligence Program," September 1, 2005
- (l) DoD Directive 5240.1, "DoD Intelligence Activities," April 25, 1988
- (m) DoD Directive 5240.2, "DoD Counterintelligence (CI)," May 22, 1997
- (n) Executive Order 12958, "Classified National Security Information," April 17, 1995, as amended
- (o) DoD Directive O-5210.41, "Security Policy for Protecting Nuclear Weapons," November 1, 2004
- (p) DoD Directive 8520.1, "Protection of Sensitive Compartmented Information (SCI)," December 20, 2001
- (q) Executive Order 12829, "National Industrial Security Program," January 6, 1993, as amended
- (r) Executive Order 12968, "Access to Classified Information," August 2, 1995
- (s) Executive Order 13356, "Strengthening the Sharing of Terrorism Information to Protect Americans," August 27, 2004
- (t) Executive Order 13354, "National Counterterrorism Center," August 27, 2004
- (u) DoD Directive S-3600.1, "Information Operations," December 9, 1996
- (v) DoD Directive S-5210.36, "Provision of DoD Sensitive Support to DoD Components and Other Departments and Agencies of the United States Government," June 10, 1986
- (w) DCID 5/1, "Coordination of United States Clandestine Foreign Activities Abroad," December 19, 1984¹
- (x) DoD Directive 5101.1, "DoD Executive Agent," September 3, 2002
- (y) DoD Directive 7045.14, "Planning, Programming, and Budgeting System," May 22, 1984
- (z) DoD 7000-14-R, "Financial Management Regulation," September 2005
- (aa) DoD Directive 5101.2, "DoD Executive Agent for Space," September 3, 2003
- (ab) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer," May 2, 2005
- (ac) DoD 5025.1-M, "DoD Directives System Procedures," March 5, 2003

¹ If a copy is needed on a need-to-know basis, contact the Office of the Under Secretary of Defense for Intelligence Staff in the Pentagon at USDI.Pubs@osd.mil.

APPENDIX 9: INTELLIGENCE LAW

DoDD 5143.01, November 23, 2005

- (ad) DoD Directive 8910.1, "Management and Control of Information Requirements," June 11, 1993

DoDD 5143.01, November 23, 2005

ENCLOSURE 2DEFINITIONS

E2.1.1. Counterintelligence. Information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (50 U.S.C. 401a)

E2.1.2. Defense Counterintelligence. Information gathered and activities conducted to detect, identify, exploit, and neutralize the intelligence capabilities and activities of terrorists, foreign powers, and other entities directed against U.S. national security.

E2.1.3. Defense Intelligence. The term “Defense Intelligence” refers to the integrated departmental intelligence that covers the broad aspects of national policy and national security and that intelligence relating to capabilities, intentions, and activities of foreign powers, organizations, or persons, including any foreign military or military-related situation or activity which is significant to Defense policy-making or the planning and conduct of military operations and activities. Defense Intelligence includes Active and Reserve military, strategic, operational, and tactical intelligence.

E2.1.4. Defense Intelligence Components. The term “Defense Intelligence Components” refers to all DoD organizations that perform national intelligence, Defense Intelligence, and intelligence-related functions, including: the Defense Intelligence Agency; the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the National Security Agency/Central Security Service, and the intelligence elements of the Active and Reserve components of the Military Departments, including the United States Coast Guard when operating as a service in the Navy.

E2.1.5. Defense Security Components. For the purposes of this Directive, the term “Defense Security Components” means all DoD organizations that perform security functions, including the Defense Security Service and the security elements of the Military Departments, including the United States Coast Guard when operating as part of the Department of the Navy, as appropriate.

E2.1.6. Defense Counterintelligence Components. For the purposes of this Directive, DoD organizations that perform national and DoD counterintelligence and counterintelligence-related functions, including the DoD Counterintelligence Field Activity and the counterintelligence elements of the Military Departments, the Defense Agencies with organic counterintelligence, the Joint Staff, the Office of the Secretary of Defense, and the Combatant Commands.

DoDD 5143.01, November 23, 2005

E2.1.7. Intelligence, Surveillance, and Reconnaissance (ISR). The term “Intelligence, Surveillance and Reconnaissance” or “ISR” refers to an activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function. (Joint Publication 1-02 as amended through November 2004)

E2.1.8. Military Intelligence. The term “Military Intelligence” refers to the collection, analysis, production, and dissemination of information relating to any foreign military or military-related situation or activity that is significant to military policy-making or the planning and conduct of military operations and activities.

E2.1.9. National Intelligence. The term “National Intelligence” refers to 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, 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. (Intelligence Reform Act of 2004, (reference (c)).

DoDD 5143.01, November 23, 2005

E3. ENCLOSURE 3

DELEGATIONS OF AUTHORITY

E3.1. Pursuant to the authority vested in the Secretary of Defense, and subject to his or her authority, direction, and control, and in accordance with DoD policies, DoD Directives, and DoD Instructions, the USD(I) is hereby delegated authority to exercise, within his or her assigned responsibilities and functional areas, all authority of the Secretary of Defense derived from statute, Executive Order, regulation, and interagency agreement, except where specifically limited by statute or Executive Order to the Secretary of Defense, including, but not limited to:

E3.1.1. Designate, on behalf of the Secretary of Defense, Department of Defense organizational elements that perform intelligence functions as Department of Defense Intelligence Components, with the concurrence of the Head of the DoD Component affected, according to Section 1614 of 10 U.S.C. In addition, the Deputy Secretary of Defense, as the head of the Office of the Secretary of Defense, delegates to the USD(I) his authority to concur in such designations for those elements and positions under the cognizance of the USD(I).

E3.1.2. Make original security classification determinations in accordance with E.O. 12958 and E.O. 12968.

E3.1.3. Carry out delegations regarding the Defense Civilian Intelligence Personnel System as prescribed in DoD Directive 1400.35 (reference (i)).

E3.1.4. Make written determinations for the conduct of all closed meetings of Federal Advisory Committees under his cognizance as prescribed by Section 10(d) of the Federal Advisory Committee Act (5 U.S.C., Appendix II, 10(d)).

E3.1.5. Make determinations relating to personal contracts for personal services that directly support the mission of a Defense Intelligence activity under 10 U.S.C. 129b(d)(1)(B).

E3.1.6. On behalf of the Secretary of Defense, waive prohibitions of award of certain contracts to entities controlled by a foreign government, according to 10 U.S.C 2536(b).

E3.2. The USD(I) may redelegate these authorities, as appropriate, and in writing, except as otherwise specifically indicated above or prohibited by law, Executive Order, DoD Directive, or regulation.

Appendix 9-2: DoDD 5240.01 – DoD Intelligence Activities

See next page.



Department of Defense
DIRECTIVE

NUMBER 5240.01
August 27, 2007

USD(I)

SUBJECT: DoD Intelligence Activities

- References:
- (a) DoD Directive 5240.1, "DoD Intelligence Activities," April 25, 1988 (hereby canceled)
 - (b) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence," November 23, 2005
 - (c) 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
 - (d) Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," October 25, 2005
 - (e) through (k), see Enclosure 1

1. REISSUANCE AND PURPOSE

This Directive:

1.1. 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)).

1.2. Updates policy and provides direction for DoD intelligence activities.

1.3. 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.

1.4. Continues to authorize the publication of DoD 5240.1-R (Reference (h)).

2. APPLICABILITY AND SCOPE

This Directive:

DoDD 5240.01, August 27, 2007

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

APPENDIX 9: INTELLIGENCE LAW

DoDD 5240.01, August 27, 2007

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.

DoDD 5240.01, August 27, 2007

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 cross-Service 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.

APPENDIX 9: INTELLIGENCE LAW

DoDD 5240.01, August 27, 2007

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.



Gordon England

Enclosures - 2

- E1. References, continued
- E2. Definitions

DoDD 5240.01, August 27, 2007

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).

DoDD 5240.01, August 27, 2007

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
- (i) 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

Appendix 9-3: DoDD 5240.1-R – Procedures Governing the Activities of DoD Intelligence Components That Affect U.S. Persons

See next page.



DoD 5240 1-R

DEPARTMENT OF DEFENSE

**PROCEDURES GOVERNING THE
ACTIVITIES OF
DOD INTELLIGENCE COMPONENTS
THAT AFFECT UNITED STATES PERSONS**

DECEMBER 1982

UNDER SECRETARY OF DEFENSE FOR POLICY

Appendix 9-4: DoDI 5210.52 – Security Classification of Airborne Sensor Imagery and Imaging Systems

See next page.

Department of Defense
INSTRUCTION

NUMBER 5210.52

May 18, 1989

ASD(C3I)

SUBJECT: Security Classification of Airborne Sensor Imagery and Imaging Systems

References: (a) DoD Instruction 5210.52, "Security Classification of Airborne Sensor Imagery," September 26, 1973 (hereby canceled)

(b) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, June 7, 1982

(c) DoD Instruction 5210.51, "Security Classification Concerning Airborne Passive Scanning Infrared Imaging Systems," September 26, 1973 (hereby canceled)

(d) DoD Instruction 5210.57, "Security Classification Concerning Airborne Radar Imaging System," September 26, 1973 (hereby canceled)

(e) through (k), see enclosure E1.

1. REISSUANCE AND PURPOSE

This Instruction:

- 1.1. Reissues reference (a) to implement revisions to reference (b).
- 1.2. Consolidates into one document references (c) and (d).
- 1.3. Updates policy, procedures, and responsibilities.

2. APPLICABILITY AND SCOPE

This Instruction:

- 2.1. Applies to the Office of the Secretary of Defense (OSD), the Military

Appendix 9-5: SECNAVINST 3820.3E – Oversight of Intelligence Activities within the Department of the Navy

See next page.



DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON, D.C. 20350-1000

SECNAVINST 3820.3E
NAVINGEN-N2
21 September 2005

SECNAV INSTRUCTION 3820.3E

From: Secretary of the Navy

Subj: OVERSIGHT OF INTELLIGENCE ACTIVITIES WITHIN THE DEPARTMENT
OF THE NAVY (DON)

Ref: (a) Executive Order 12333
(b) DOD Directive 5240.1 of 25 Apr 88
(c) DOD Regulation 5240.1-R of Dec 82
(d) SECNAVINST 5000.34B
(e) DOD Directive 5148.11
(f) SECNAVINST 5510.30A
(g) US Navy Regulations, 1990
(h) SECNAVINST 5215.1D, Secretary of the Navy Directives
Policy

Encl: (1) Naval Inspector General Intelligence Oversight
Inspection Checklist
(2) Naval Inspector General Intelligence Oversight
Report Format and Content
(3) Memorandum of Understanding: Reporting of Information
Concerning Federal Crimes, August 1995

1. Purpose. To implement policies, procedures, and governing regulations regarding the conduct of intelligence activities, and a system of program reviews, inspections, and reporting requirements of those activities. This instruction has been substantially revised and should be reviewed in its entirety. Highlights of significant changes from previous instruction are as follows:

a. Updated definition of "DON intelligence components," - to include new and reorganized DON intelligence organizations and describe revised responsibilities under this instruction,

b. Further definition of the term "Questionable intelligence activity" and resultant reporting requirements (i.e. Procedure 15 reporting),

c. Inclusion of a sample Intelligence Oversight inspection checklist, which may be used by components or elements as a guideline for administering an effective Intelligence Oversight program, (enclosure (1)), and

d. Inclusion of a standard format for quarterly reports from DON intelligence components to the Office of the Naval Inspector General (NAVINGEN) (enclosure (2)).

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E

21 September 2005

2. Cancellation. SECNAVINST 3820.3D.

3. Background.

a. Intelligence Oversight ensures that all tasks performed by intelligence, counterintelligence, and intelligence related activities are conducted in accordance with Federal law, Executive Orders, DOD directives, regulations and policies.

b. The collection, retention, and dissemination of information concerning U.S. persons and the conduct of intelligence activities by Department of the Navy (DON) intelligence components will be governed by the requirements set forth in references (a) through (c), enclosure (3), and this instruction.

c. The Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)) is responsible for developing Intelligence Oversight policy within the Department of Defense (DOD) consistent with references (a) through (c).

4. Scope and Applicability. This instruction applies to all DON intelligence components and governs all intelligence activities undertaken by personnel assigned to those components. This instruction also applies to non-intelligence personnel, engaged in any intelligence activity (e.g., collection, research, analysis, production, retention, dissemination), as well as all other DON components and personnel when that component conducts intelligence and/or intelligence-related activities. This instruction does not apply to law enforcement activities carried out by DON law enforcement agencies that also have an intelligence mission. It does not constitute authority for any DON intelligence component to conduct an activity not otherwise authorized by law. Questions of interpretation pertaining to references (a), (b), (c) or this instruction should be referred to the legal office responsible for advising the component concerned. If such questions are not resolved at that level, they should be taken up that component's legal chain of command for resolution and, if necessary, to the General Counsel of the Navy or to the Judge Advocate General, depending on which office would otherwise have cognizance over the issue. Alternatively, such questions may also be referred to the Office of the Naval Inspector General (NAVINSGEN), who may refer this matter to the General Counsel of the Navy (GC), the Judge Advocate General (JAG), or the General Counsel of the Department of Defense (DODGC) for resolution, as appropriate. If a question is referred to the component's legal chain of command for resolution, that office shall keep NAVINSGEN informed of the status of the review, and any conclusions reached or advice rendered in connection with such question(s). Likewise, if a

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E
21 September 2005

question is referred to NAVINSGEN for resolution, that office shall keep the component's cognizant legal office informed of the status of the review, and any conclusions reached or advice rendered in connection with such question(s). Requests for exceptions or amendments to the policies or procedures issued by this instruction should be referred to NAVINSGEN.

5. Conduct of Intelligence Activities.

a. DON intelligence components and personnel shall carry out their authorized missions and functions per the policies and procedures contained in references (a), (b), (c), and this instruction. Moreover, they shall carry out their authorized functions in a manner that does not violate the constitutional rights and privacy of U.S. persons, and shall not request any other person or entity to undertake unauthorized activities. Use of the techniques prescribed by reference (c) to collect information about U.S. persons shall be accomplished by the least intrusive means practicable.

b. DON personnel shall not conduct, or provide support for the conduct of, special activities without proper authorization, and will comply with the reporting requirements of higher authority. Reference (d) provides guidance for the conduct and oversight of intelligence, intelligence-related, special, and sensitive activities within the DON.

c. Under no circumstances shall any DON personnel condone, support, encourage, engage in, or conspire to engage in the assassination of a specific individual or individuals.

6. Action.

a. NAVINSGEN shall submit to ATSD(IO), with a copy each to JAG, CNO (N2) GC, and UNSECNAV, a quarterly Intelligence Oversight report for the Department of the Navy describing:

(1) Any intelligence or counterintelligence activity that has come to the attention of NAVINSGEN during the quarter reasonably believed to be illegal, improper, or contrary to references (a), (b), (c), this instruction, or other applicable directives, and policies. The report may also include any corrective action taken, as appropriate.

(2) Any significant Intelligence Oversight activities undertaken during the quarter (i.e., inspections, training, published documents).

(3) Any recommendations for improvement to existing Intelligence Oversight regulations and the subject program.

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E
21 September 2005

(4) Status of any outstanding reports of confirmed or suspected questionable intelligence activity.

b. DON intelligence components, less USMC intelligence components, shall submit to NAVINSGEN a quarterly Intelligence Oversight report for their respective component (and claimancy) covering the information identified in paragraph 6.a. above. USMC elements shall submit to DNIGMC a quarterly Intelligence Oversight report similarly covering the information identified in paragraph 6.a. above. DNIGMC shall then submit a consolidated report to NAVINSGEN on behalf of all USMC elements.

(1) The format for DON intelligence component and DNIGMC quarterly Intelligence Oversight reports is provided in enclosure (2).

(2) Significant instances of fraud, waste, abuse, standards of conduct or ethics violations (less that described above), financial misconduct, or conflicts of interest that affect intelligence operations do not need to be included in the quarterly Intelligence Oversight reports. However, they shall be reported to NAVINSGEN, as appropriate, via a separate report, e-mail, or Hotline action.

c. Commanding Generals and Inspectors General of Fleet Marine Forces will comply with the above reporting requirements and submit their quarterly Intelligence Oversight report to DNIGMC, as directed.

d. Quarterly Intelligence Oversight reporting periods and report due dates are identified as follows:

<u>QUARTER</u>	<u>REPORT DUE TO NAVINSGEN</u>
First Quarter (JAN/FEB/MAR)	15 APR
Second Quarter (APR/MAY/JUN)	15 JUL
Third Quarter (JUL/AUG/SEP)	15 OCT
Fourth Quarter (OCT/NOV/DEC)	15 JAN

7. Definitions. The following terms are used throughout this instruction.

a. DON intelligence components include:

- (1) The Office of the Director of Naval Intelligence (CNO (N2)),
- (2) The Office of Naval Intelligence (ONI),
- (3) Naval Security Group Command (NAVSECGRU),

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E
21 September 2005

(4) Naval Criminal Investigative Service (NCIS) (specifically those select elements of NCIS conducting counterintelligence activities),

(5) Marine Corps intelligence components,

(6) Naval Reserve Intelligence Program (CNRIC),

(7) Naval Security Group Command Reserve (CNSGR),

(8) Other DON organizations, staffs, and offices, when used for foreign intelligence or counterintelligence activities, including command and subordinate intelligence staffs, activities, units, and elements of Commander, Fleet Forces Command (COMFLTFORCOM); Commander U.S. Pacific Fleet (COMPACFLT); Commander, U.S. Naval Forces Central Command (COMUSNAVCENT); Commander, U.S. Naval Forces Southern Command (COMUSNAVSO); Commander, U.S. Naval Forces Europe/Commander, U.S. Sixth Fleet (COMUSNAVEUR/COMSIXTHFLT); Commander, Naval Reserve Force (COMNAVRESFOR); Commander, Naval Special Warfare Command (COMNAVSPECWAR); and Echelon 2, 3, 4, 5, and 6 commands that do not report operationally or administratively for Intelligence Oversight reporting and inspection purposes to any of the other DON intelligence components defined in subparagraph 7a(1) through 7a(8). The heads of such organizations, staffs, and offices listed in this subparagraph shall not be considered heads of DOD intelligence components for the purposes of approving intelligence collection activities authorized by references (c) and (d).

b. Marine Corps Intelligence components, for purposes of Intelligence Oversight, include the Office of the Director of Intelligence, Headquarters U.S. Marine Corps (HQMC-I), Marine Corps Intelligence Activity (MCIA), Marine Corps intelligence units, G-2/S-2 staffs, intelligence battalions, radio battalions, reconnaissance battalions/companies, scout sniper platoons, unmanned aerial vehicle squadrons, and Marine Corps reserve counterparts.

c. Intelligence activity is the collection, production and dissemination of foreign intelligence and counterintelligence by DON intelligence components.

d. Intelligence-related activities are activities normally considered to be linked directly or indirectly to the intelligence field.

e. Questionable intelligence activity is intelligence that may violate Federal law, an Executive Order (such as EO 12333), a Presidential Directive, DON policies, or this instruction.

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E
21 September 2005

Examples of questionable intelligence activity include, but are not limited to, the following:

(1) Tasking intelligence personnel to conduct intelligence activities that are not part of the organization's approved mission, even if they have the technical capability to do so.

(2) Providing intelligence services and/or products without proper authorization.

(3) Failing to file proper use statement for imagery collection associated with U.S. persons.

(4) Collecting information on U.S. persons, even through open source, when it is not part of the unit's mission.

f. Special activities as defined by reference (a) are activities conducted in support of national foreign policy objectives abroad which are planned and executed so the role of the U.S. Government is not apparent or acknowledged publicly, and functions in support of such activities, but which are not intended to influence U.S. political processes, public opinion, policies, or media and do not include diplomatic activities or the collection and production of intelligence or related support functions.

g. Other terms used in this instruction are defined in references (b) through (d).

8. Violations. This instruction at paragraphs 5.b. and 5.c., reference (a) at parts 2.3, 2.4, and 2.9 through 2.12, and reference (c) at chapters 1 through 15 constitute and shall apply as general regulatory orders. They apply to all eligible DON personnel individually and need no further implementation. A violation of those provisions is punishable under the Uniform Code of Military Justice for military personnel and may be the basis for appropriate administrative disciplinary procedures with respect to civilian employees.

9. Intelligence Oversight Responsibilities.

a. The Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and the General Counsel of the Navy for NCIS shall:

(1) Implement the policies and procedures contained in references (a), (b), (c), and this instruction.

(2) Ensure the Under Secretary of the Navy (UNSECNAV),

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E

21 September 2005

GC, JAG, NAVINSGEN, and the Senior Review Board (SRB), are kept fully and currently informed of significant and/or sensitive DON intelligence activities, questionable intelligence activities, and intelligence-related activities using any DON non-intelligence component assets, including personnel and equipment. In those instances where DON intelligence components support National Security Agency (NSA) activities, those activities need not be reported under the provisions of this subparagraph when they are subject to the current Intelligence Oversight activities of NSA. Nothing in this subparagraph is intended to exempt DON intelligence activities from complying with any separate non-Intelligence Oversight related, reporting requirement.

(3) Ensure NAVINSGEN is notified each time any Navy or Marine Corps organization, staff, or office not specifically identified as a DON intelligence component in paragraphs 7.a. and 7.b. of this instruction is tasked to collect, retain, or disseminate information for intelligence or counterintelligence purposes.

b. Heads of DON intelligence components and elements thereof, as appropriate, shall:

(1) Ensure that all subordinate intelligence components, activities, units, and elements in or under their command comply with the requirements of references (a), (b), (c), and this instruction.

(2) Report to NAVINSGEN within 48 hours confirmed or suspected questionable intelligence activities conducted by or on behalf of their respective component (reference (c), chapter 15, germane).

(3) Report to NCIS any possible federal crimes by employees of DON intelligence organizations, or violations of specified federal criminal laws by any other person when collected as part of intelligence activities as required in enclosure (3).

(4) Ensure that all intelligence activities, in whole or in part, which raise issues of legality, consistency with applicable policy, or propriety in general are submitted for legal review prior to implementation or as soon as identified. Navy and Marine Corps command or staff judge advocates or Office of the General Counsel attorneys of the component concerned, who possess the requisite security clearances, shall participate actively in the operational planning and review of intelligence activities. Activities or legal issues of significance should be referred to the legal office responsible for advising the component concerned. If such issues are not resolved at that

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E

21 September 2005

level, they should be taken up that component's legal chain of command for resolution and, if necessary, to the General Counsel of the Navy or to the Judge Advocate General, depending on which office would otherwise have cognizance over the issue. Alternatively, such issues may also be referred for review to NAVINSGEN, who may refer the matter to and confer with the GC, JAG, or DODGC, as appropriate. Marine Corps issues shall be referred via the Counsel for the Commandant, Staff Judge Advocate to the Commandant, and Deputy Naval Inspector General for Marine Corps Matters (DNIGMC), as appropriate. If an issue or question is referred to the component's legal chain of command for resolution, that office shall keep NAVINSGEN informed of the status of the review, and any conclusions reached or advice rendered in connection with such issue(s) or question(s). Likewise, if an issue or question is referred to NAVINSGEN for resolution, that office shall keep the component's cognizant legal office informed of the status of the review, and any conclusions reached or advice rendered in connection with such issue(s) or question(s).

(5) Ensure Intelligence Oversight refresher training of all staff and subordinate DON personnel is conducted and documented on an annual basis. Intelligence components are not required to train personnel who are not involved in the intelligence mission of the command (e.g., Morale, Welfare, and Recreation employees, groundskeepers, etc.). At a minimum, annual refresher training shall familiarize employees with the provisions of references (a), (b), (c), and this instruction that apply to the operations and activities of their component, and of their responsibilities under this instruction to report suspected or confirmed questionable intelligence activities.

(6) Ensure that no adverse or retaliatory action is taken against any personnel who reports confirmed or suspected questionable intelligence activities under this instruction.

(7) Ensure that employees and contractors assigned to a DON intelligence component and who are aware of the intelligence mission of the component, shall:

(a) Familiarize themselves with the policies and procedures required by this instruction and references (a), (b), and (c).

(b) Report suspected or confirmed questionable intelligence activities to the Inspector General of the command or intelligence component concerned, NAVINSGEN, GC, JAG, DNIGMC, Staff Judge Advocate to the Commandant, Counsel for the Commandant (for Marine Corps matters), DODGC, or ATSD(IO), as appropriate. If it is not practical to report through the chain

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E
21 September 2005

of command, an employee may report questionable intelligence activity directly to the office of the NAVINSGEN.

(8) Impose such sanctions as may be appropriate on any employee who violates the provisions of references (a), (b), (c), and this instruction.

(9) Ensure NAVINSGEN, GC, JAG, DNIGMC, Counsel for the Commandant, Staff Judge Advocate to the Commandant (for Marine Corps Matters), DODGC, and ATSD(IO), as appropriate and after proper security clearance is verified, have access to all information concerning intelligence activities in the conduct of Intelligence Oversight responsibilities, and that employees of their components cooperate fully with such officials.

(10) Provide to NAVINSGEN annually, no later than (NLT) 15 September, an updated list of all intelligence component activities, units and elements in or under their command. The list shall include the full address for each command/activity/unit/element, as well as the date of the most recent Intelligence Oversight inspection by the lead echelon. A summary of modifications identifying any commands/activities/units/elements to be added or deleted (compared to previous year's list) shall also be included along with a brief justification for the change(s). Marine Corps Intelligence components will provide their input to DNIGMC.

(11) Provide to NAVINSGEN annually, (NLT) 15 September, a schedule of Intelligence Oversight inspections to be conducted during the upcoming fiscal year for all components, activities, units, and elements under their command.

(12) Conduct Intelligence Oversight inspections on all subordinate shore intelligence components, activities, units, and elements in or under their command at an interval of no greater than once every 36 months, with appropriate follow-up/"spot checks" or assistance between inspections as deemed necessary.

(13) Provide a quarterly Intelligence Oversight report to NAVINSGEN as directed in paragraph 6. DNIGMC will consolidate report inputs from Marine Corps intelligence components and provide a single Marine Corps quarterly Intelligence Oversight report input to NAVINSGEN for incorporation into subsequent reporting to ATSD(IO).

(14) Intelligence oversight inspections are not required for afloat activities (e.g. squadrons, ships, and submarines). Nonetheless, Commanding Officers remain accountable for annual Intelligence Oversight training, reporting of that training to appropriate higher authority (identified subparagraph 7.a).

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E
21 September 2005

above), and active enforcement of intelligence oversight matters. As well, should an Intelligence Oversight infraction or a suspected questionable activity occur while afloat, it must be reported to higher authority.

c. NAVINSGEN shall be responsible for:

(1) Inspecting DON intelligence components to ensure compliance with references (a), (b), (c), and this instruction. Of note, although COMSIXTHFLT would normally be exempt, subject merger of duties and responsibilities with COMUSNAVEUR staff mandate that the combined staff is fully accountable for all Intelligence Oversight program requirements, including periodic inspection. (Enclosure (1) will be used by NAVINSGEN as a baseline checklist during inspection of component Intelligence Oversight programs.)

(2) Investigating reports of confirmed or suspected questionable intelligence activities. Suspected criminal activities will be referred to NCIS for investigation.

(3) Investigating any alleged failures of DON intelligence components to report confirmed or suspected questionable intelligence activities. In the event that questionable intelligence activities are conducted by, or on behalf of, a DON intelligence component but not reported, NAVINSGEN will recommend appropriate corrective action.

(4) Ensuring procedures exist within all DON intelligence components for the reporting of questionable intelligence activities, and for documenting that employees of DON intelligence components are familiar with the provisions of references (a), (b), and (c), and are aware of their responsibilities to report questionable intelligence activities.

(5) Referring reports of confirmed or suspected questionable intelligence activities to the GC, or JAG, as appropriate, to determine whether the activity is legal and consistent with applicable policy.

(6) Immediately reporting to the DODGC and ATSD(IO) questionable intelligence activities of a serious nature.

(7) Carrying out other Intelligence Oversight responsibilities set forth in references (a) through (e), and this instruction.

d. The Deputy Naval Inspector General for Marine Corps Matters (DNIGMC) shall be responsible for carrying out the functions outlined in subparagraph 9.c., with respect to Marine

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E
21 September 2005

Corps intelligence component activities, units, and elements and report subject results to NAVINSGEN.

e. The General Counsel of the Navy, in coordination with the Judge Advocate General, shall be responsible for:

(1) Determining whether activities, as defined in paragraph 7 of this instruction, conducted by DON intelligence components, are in compliance with applicable law and regulations.

(2) Referring reports of suspected or confirmed questionable intelligence activities conducted by or on behalf of DON intelligence components to NAVINSGEN for investigation.

(3) Carrying out any applicable responsibilities as set forth in references (a) through (c) and enclosure (3).

10. Reports. Reports required by this instruction are exempt from reports control per SECNAVINST 5214.2B.

11. Authority. References (g) and (h) authorize the Naval Inspector General to issue this instruction and publish changes to it.



R. A. ROUTE
Vice Admiral, U.S. Navy
Naval Inspector General

Distribution:
Electronic only, via Navy Directives Website at
<http://ned.s.daps.dla.mil//>

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E
21 September 2005

Naval Inspector General Intelligence Oversight Inspection Checklist

ACTIVITY/DETACHMENT: _____

POINT(S) OF CONTACT: _____

TODAY'S DATE: _____

INSPECTOR(S): _____

Definition of terms: For purposes of this checklist, the term Executive Order 12333 compliance shall include compliance/ noncompliance with, or violations of, Executive Order 12333 and DOD Regulation 5240.1-R of December 1982 (NOTAL) as well as unauthorized intelligence missions and functions.

1. Intelligence Oversight Policy

a. Does the Commanding Officer, Executive Officer, Officer in Charge and Senior Intelligence Officer receive annual training on Executive Order 12333 and its DOD and Navy implementing directives/regulations/instructions?

b. Describe the command's Intelligence Oversight program.

c. What are the training, inspection, and reporting mechanisms?

d. Have any violations occurred? If so, when and how reported? What corrective actions were taken?

e. What is the impact of Intelligence Oversight restrictions on the command's mission?

f. Is the official responsible for administering the command's Intelligence Oversight program designated by command instruction (Intelligence Oversight instruction, Standards Operations Regulations Manual, collateral duty list) or designation letter?

g. Does this official have access to all the intelligence collection, retention (databases, files), and dissemination programs within the command for oversight purposes?

h. If not, what mechanism is in place to ensure compliance with Executive Order 12333?

Enclosure (1)

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E
21 September 2005

i. Who certifies compliance with Executive Order 12333 for all command programs? How is compliance for all programs certified to this official?

NOTE: Reports will be sent/forwarded to Echelon 2 if inspecting Echelon 3 or below. Is the quarterly report to NAVINSGEN signed by direction? Who signs? What is the command relationship to the official who certifies compliance?

j. Has the command received any tasking from higher authority that could actually or potentially (or perceived to be) contrary to intelligence restrictions? How was it handled? What was the outcome? How was it documented?

2. Training and Compliance Elements

a. Does the command hold SECNAVINST 3820.3E? DOD Directive 5240.1? DOD Regulation 5240.1-R? Executive Order 12333?

b. Does the command have its own instruction on Intelligence Oversight?

c. Does the command instruction or directive designate the official responsible for conducting/coordinating Intelligence Oversight training?

d. Does the command have NAVINSGEN-N2 (or the appropriate Echelon 2) POC's phone numbers, e-mail addresses and Internet home page address (as applicable)? Do they have the Navy Hotline number? DODIG phone number? ATSD(IO) phone number?

e. How is required annual training conducted and documented? (Review training records for the last 3 years)

f. How does the command review its programs for compliance with Executive Order 12333? How are the results documented? How frequently are programs reviewed?

g. Are contracting activities reviewed for Executive Order 12333 compliance?

h. Are espionage cases reported to NAVINSGEN quarterly per SECNAVINST 3820.3E?

i. Are significant instances of fraud, waste, abuse, standards of conduct or ethics violations, financial misconduct, or conflicts of interest that impact upon intelligence operations reported to senior echelon or NAVINSGEN quarterly (per SECNAVINST 3820.3E)?

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E
21 September 2005

j. What databases does the command have access to that contain information on U.S. persons? How is compliance with Executive Order 12333 ensured? Are there directives or SOPs for preventing Executive Order 12333 violations when accessing these databases?

k. What is the reporting procedure for personnel to report questionable activities?

l. Is the proper channel for reporting Executive Order 12333 violations well publicized within the Command?

NOTE: Are Plan of the Day notes run periodically? Are notices posted on bulletin boards? Are the Executive Officer, Command Master Chief, military Division Officers, and senior civilians conversant with the procedures for reporting Executive Order 12333 violations?

m. Are there any command personnel assigned independent duty or serving in outlying areas? If so, how is Intelligence Oversight training administered? How is Executive Order 12333 compliance monitored and documented?

n. How do personnel receive Intelligence Oversight training when they report aboard? Is it part of the check-in process?

o. How does the command ensure subcomponents are inspected per the timelines established in SECNAVINST 3820.3E? Is an oversight inspection schedule submitted to NAVINSGEN each September per SECNAVINST 3820.3E? Are inspection records current?

3. Potential Problem Areas

- a. Are there any indications of:
1. Potential oversight violations?
 2. Standards of Conduct problems?
 3. Fraud/waste/abuse
 4. Financial misconduct?
 5. Conflict of interest?
 6. Espionage?
 7. Violation of law, directives, policy, or procedures?

- b. Have any of the following special collection techniques been used by the command:
1. Concealed monitoring?
 2. Physical searches?
 3. Searches and examinations of mail?
 4. Physical surveillance?

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E

21 September 2005

5. Undisclosed participation in organizations to gain intelligence information?

4. Personnel and Records Review

- a. Visit operating spaces and randomly question personnel to evaluate their knowledge of intelligence activities.

- b. Examine intelligence files for compliance with collection and retention criteria.

- c. Is the annual training required by SECNAVINST 3820.3E reported in a timely manner by subordinate commands? How are they monitored by the Echelon 2 command?

5. Command Feedback. Does the command have any recommendations for improving the Intelligence Oversight process?

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E
21 September 2005

Naval Inspector General
Intelligence Oversight Report (Format and Content)

3820
Ser/

From: Reporting Command
To: Naval Inspector General (ATTN: N2)
Subj: QUARTERLY INTELLIGENCE OVERSIGHT REPORT FOR __ QUARTER/
FISCAL YEAR __
(e.g. QUARTERLY INTELLIGENCE OVERSIGHT REPORT FOR
4RD QUARTER/FISCAL YEAR 2005)
Ref: (a) SECNAVINST 3820.3E

1. Per reference (a), the following report is provided.
2. (In paragraph 2, identify any subordinate commands that were inspected during the quarter in the following format.)

e.g. The following Intelligence Oversight inspections were conducted during this quarter:

<u>COMMAND</u>	<u>INSPECTION DATE</u>
Command Alfa	12 AUG 05
Command Bravo Det One	15 AUG 05

3. (In paragraph 3, discuss any significant Intelligence Oversight program-related activities that occurred during this quarter - e.g. training initiatives, awareness, indoctrination, familiarization, published documents, new instructions or policy.)
4. (In paragraph 4, identify/discuss any recommendations (if any) as to how the Intelligence Oversight system or overall program may be improved.)
5. (In paragraph 5, provide a statement describing those activities (if any) that have come to the attention of the command during subject quarter, which are reasonably believed to be illegal or contrary to Executive Order or Presidential directive, or applicable DOD policy. Be sure to include an explanation of all action(s) taken at all levels, as applicable, with respect to such activities.)

Enclosure (2)

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E
21 September 2005

6. (In paragraph 6, provide a statement describing the status of any earlier (outstanding) reports of confirmed or suspected questionable intelligence activity that have already been reported during a previous quarter.)

7. (In paragraph 7, identify your command Intelligence Oversight point of contact - to include command representative/name, phone number, fax number and e-mail address, if available.)

Y.R. SIGNATURE

SECNAVINST 3820.3E
21 September 2005

MEMORANDUM OF UNDERSTANDING:
REPORTING OF INFORMATION CONCERNING FEDERAL CRIMES

I. Introduction

Section 1.7(a) of Executive Order (E.O.) 12333 requires senior officials of the Intelligence Community to -

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 or agency concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures.

Title 28, United States Code, Section 535(b) requires that

[a]ny information, allegation, or complaint received in a department or agency of the executive branch of the Government relating to violations of title 18 involving Government officers and employees shall be expeditiously reported to the Attorney General by the head of the department or agency, unless -

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

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

This Memorandum of Understanding (MOU) sets forth the procedures by which each agency and organization within the Intelligence Community shall report to the Attorney General and to federal investigative agencies information concerning possible federal crimes by employees of an intelligence agency or organization, or violations of specified federal criminal laws by any other person, which information was collected by it during the performance of its designated intelligence activities, as those activities are defined in E.O. 12333, §§ 1.8-1.13.

II. Definitions

A. "Agency," as that term is used herein, refers to those agencies and organizations within the Intelligence Community as defined in E.O. 12333, § 3.4(f), but excluding the intelligence elements of the Federal Bureau of Investigation and the Department of the Treasury.

B. "Employee," as that term is used herein, means:

1. a staff employee, contract employee, asset, or other person or entity providing service to or acting on behalf of any agency within the intelligence community;
2. a former officer or employee of any agency within the

Enclosure (3)

SECNAVINST 3820.3E
21 September 2005

intelligence community for purposes of an offense committed during such person's employment, and for purposes of an offense involving a violation of 18 U.S.C. § 207 (Conflict of interest); and

3. any other Government employee on detail to the Agency.

- C. "General Counsel" means the general counsel of the Agency or of the Department of which it is a component or an oversight person designated by such person to act on his/her behalf, and for purposes of these procedures may include an Inspector General or equivalent official if agency or departmental procedures so require or if designated by the agency or department head.
- D. "Inspector General" or "IG" means the inspector general of the Agency or of the department of which the Agency is a component.
- E. "Reasonable basis" exists when there are facts and circumstances, either personally known or of which knowledge is acquired from a source believed to be reasonably trustworthy, that would cause a person of reasonable caution to believe that a crime has been, is being, or will be committed. The question of which federal law enforcement or judicial entity has jurisdiction over the alleged criminal acts shall have no bearing upon the issue of whether a reasonable basis exists.

III. Scope

- A. This MOU shall not be construed to authorize or require the Agency, or any person or entity acting on behalf of the Agency, to conduct any investigation not otherwise authorized by law, or to collect any information in a manner not authorized by law.
- B. This MOU ordinarily does not require an intelligence agency or organization to report crimes information that was collected and disseminated to it by another department, agency, or organization. Where, however, the receiving agency is the primary or sole recipient of that information, or if analysis by the receiving agency reveals additional crimes information, the receiving agency shall be responsible for reporting all such crimes information in accordance with the provisions of this MOU.
- C. This MOU does not in any way alter or supersede the obligation of an employee of an intelligence agency to report potential criminal behavior by other employees of that agency to an IG, as required either by statute or by agency regulations, nor affect any protections afforded any persons reporting such behavior to an IG. Nor does this MOU affect any crimes reporting procedures between the IG Offices and the Department of Justice.
- D. This MOU does not in any way alter or supersede any obligation of a department or agency to report to the Attorney General criminal behavior by Government employees not employed by the intelligence community, as required by 28 USC §535.

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E
21 September 2005

- E. This MOU does not affect the obligation to report to the Federal Bureau of Investigation alleged or suspected espionage activities as required under Section 811(c) of the Intelligence Authorization Act of 1995.
- F. The following crimes information is exempted from the application of this memorandum if the specified conditions are met:
1. Crimes information that has been reported to an IG;¹
 2. Crimes information received by a Department of Defense intelligence component concerning a Defense intelligence component employee who either is subject to the Uniform Code of Military Justice or is a civilian and has been accused of criminal behavior related to his/her assigned duties or position, if (a) the information is submitted to and investigated by the appropriate Defense Criminal Investigative Organization, and (b) in cases involving crimes committed during the performance of intelligence activities, the General Counsel provides to the Department of Justice a report reflecting the nature of the charges and the disposition thereof;
 3. Information regarding non-employee crimes listed in Section VII that is collected by the intelligence component of a Department also having within it a law enforcement organization where (a) the crime is of the type that the Department's law enforcement organization has jurisdiction to investigate; and (b) the Department's intelligence organization submits that crimes information to the Department's law enforcement organization for investigation and further handling in accordance with Department policies and procedures.²
 4. Crimes information regarding persons who are not employees of the Agency, as those terms are defined in Section II, that involve crimes against property in an amount of \$1,000 or less, or, in the case of Agency employees, crimes against property in an amount of \$500 or less. As to other relatively minor offenses to which this MOU would ordinarily apply, but which, in the General Counsel's opinion, do not warrant reporting pursuant to this MOU, the General Counsel may

¹ If, however, the IG determines that the reported information is not properly subject to that office's jurisdiction, but that such information may be reportable pursuant to this MOU, the IG may forward the information to the DOJ in compliance with these procedures. Alternatively, the IG may transmit the information to the Agency's General Counsel for a determination of what response, if any, is required by this MOU.

² This MOU does not affect the crimes reporting obligations of any law enforcement and other non-intelligence components of a department, agency, or organization.

SECNAVINST 3820.3E
21 September 2005

orally contact the Assistant Attorney General, Criminal Division, or his/her designee. If the Department of Justice concurs with that opinion, no further reporting under these procedures is required. The General Counsel shall maintain an appropriate record of such contacts with the Department. If deemed appropriate by the General Counsel, he/she may take necessary steps to pass such information to the appropriate law enforcement authorities; or

5. Information, other than that relating to homicide or espionage, regarding crimes that were completed more than ten years prior to the date such allegations became known to the Agency. If, however, the Agency has a reasonable basis to believe that the alleged criminal activities occurring ten or more years previously relate to, or are a part of, a pattern of criminal activities that continued within that ten year interval, the reporting procedures herein will apply to those activities.
- F. The procedures set forth herein are not intended to affect whether an intelligence agency reports to state or local authorities activity that appears to constitute a crime under state law. In the event that an intelligence agency considers it appropriate to report to state or local authorities possible criminal activity that may implicate classified information or intelligence sources or methods, it should inform the AAG, or the designated Deputy AAG, Criminal Division, in accordance with paragraph VIII.C, below; the Criminal Division will consult with the intelligence agency regarding appropriate methods for conveying the information to state or local authorities. In the event that an intelligence agency considers it appropriate to report to state or local authorities possible criminal activity that is not expected to implicate classified information or intelligence sources or methods, it should nevertheless provide a copy of such report to the AAG, or to the designated Deputy AAG, Criminal Division.

IV. General Considerations: Allegations of Criminal Acts Committed By Agency Employees

- A. This Agreement requires each employee of the Agency to report to the General Counsel or IG facts or circumstances that reasonably indicate to the employee that an employee of an intelligence agency has committed, is committing, or will commit a violation of federal criminal law.³

³ When a General Counsel or IG has received information concerning alleged violations of federal law by an employee of another intelligence community agency, and those violations are not exempted under section III.E.4, hereof, the General Counsel shall notify in writing the General Counsel of the accused employee's agency. The latter General Counsel must then determine whether this MOU requires the allegations to be reported to the Department of Justice.

SECNAVINST 3820.3E
21 September 2005

- B. Except as exempted in Section III, when the General Counsel has received allegations, complaints or information (hereinafter allegations) that an employee of the Agency may have violated, may be violating, or may violate a federal criminal statute, that General Counsel should within a reasonable period of time determine whether there is a reasonable basis to believe that a federal crime has been, is being, or will be committed and that it is a crime which, under this memorandum, must be reported. The General Counsel may, as set forth in Section V, below, conduct a preliminary inquiry for this purpose. If a preliminary inquiry reveals that there is a reasonable basis for the allegations, the General Counsel will follow the reporting procedures set forth in Section VIII, below. If a preliminary inquiry reveals that the allegations are without a reasonable basis, the General Counsel will make a record, as appropriate, of that finding and no reporting under these procedures is required.
- V. Preliminary Inquiry Into Allegations Against an Agency Employee
- A. The General Counsel's preliminary inquiry regarding allegations against an Agency employee will ordinarily be limited to the following:
1. review of materials submitted in support of the allegations;
 2. review of Agency indices, records, documents, and files;
 3. examination of premises occupied by the Agency;
 4. examination of publicly available federal, state, and local government records and other publicly available records and information;
 5. interview of the complainant; and
 6. interview of any Agency employee, other than the accused, who, in the opinion of the General Counsel, may be able to corroborate or refute the allegations.
- B. Where criminal allegations against an Agency employee are subject to this MOU, an interview of that employee may only be undertaken in compliance with the following conditions:
1. Where the crime alleged against an Agency employee does not pertain to a serious felony offense,⁴ a responsible Agency

⁴ A "serious felony offense" includes any offense listed in Section VII, hereof, violent crimes, and other offenses which, if committed in the presence of a reasonably prudent and law-abiding person, would cause that person immediately to report that conduct directly to the police. For purposes of this MOU, crimes against government property that do not exceed \$5,000 and are not part of a pattern of continuing behavior or of a criminal conspiracy shall not be considered serious felony offenses.

SECNAVINST 3820.3E
21 September 2005

official may interview the accused employee; however, such interview shall only be conducted with the approval of the General Counsel, the IG, or, as to Defense and military employees, the responsible military Judge Advocate General or the responsible Defense Criminal Investigative Organization.

2. Where the crime alleged against an Agency employee is a serious felony offense, the Agency shall ordinarily not interview the accused employee, except where, in the opinion of the General Counsel, there are exigent circumstances⁵ which require that the employee be interviewed. If such exigent circumstances exist, the General Counsel or other attorney in the General Counsel's office may interview the accused employee to the extent reasonably necessary to eliminate or substantially reduce the exigency.
3. In all other cases of alleged serious felonies, the General Counsel, or the General Counsel's designee, may interview the accused employee only after consultation with the Agency's IG, a Defense Criminal Investigative Organization (for Defense and military employees), or with the Department of Justice regarding the procedures to be used during an interview with the accused employee.

Any interview of an accused employee that is undertaken shall be conducted in a manner that does not cause the loss, concealment, destruction, damage or alteration of evidence of the alleged crime, nor result in the immunization of any statements made by the accused employee during that interview. The Agency shall not otherwise be limited by this MOU either as to the techniques it is otherwise authorized to use, or as to its responsibility to provide for its security functions pursuant to E.O. 12333.

VI. General Considerations: Allegations Of Criminal Acts Committed By Non-Employees

- A. This MOU requires each employee of the Agency to report, to the General Counsel or as otherwise directed by the Department or Agency head, facts or circumstances that reasonably indicate to the employee that a non-employee has committed, is committing, or will commit one or more of the specified crimes in Section VII, below.
- B. When an Agency has received information concerning alleged violations of federal law by a person other than an employee of an intelligence agency, and has determined that the reported information provides a reasonable basis to conclude that a violation of one of the specified crimes in Section VII has occurred, is

⁵ "Exigent circumstances" are circumstances requiring prompt action by the Agency in order to protect life or substantial property interests; to apprehend or identify a fleeing offender; or to prevent the compromise, loss, concealment, destruction, or alteration of evidence of a crime.

SECNAVINST 3820.3E
21 September 2005

occurring, or may occur, the Agency shall report that information to the Department of Justice in accordance with Sections VIII or IX, below.

VII. Reportable Offenses by Non-Employees

- A. Unless exempted under Section III, above, allegations concerning criminal activities by non-employees are reportable if they pertain to one or more of the following specified violations of federal criminal law:
1. Crimes involving intentional infliction or threat of death or serious physical harm. These include but are not limited to homicide, kidnapping, hostage taking, assault (including sexual assault), or threats or attempts to commit such offenses, against any person in the United States or a U.S. national or internationally protected person (as defined in 18 U.S.C. § 1116(b)(4)), whether in the United States or abroad.
 2. Crimes, including acts of terrorism, that are likely to affect the national security, defense or foreign relations of the United States. These may include but are not limited to:
 - a. Espionage; sabotage; unauthorized disclosure of classified information; seditious conspiracies to overthrow the government of the United States; fund transfers violating the International Emergency Economic Powers Act; providing material or financial support to terrorists; unauthorized traffic in controlled munitions or technology; or unauthorized traffic in, use of, or contamination by nuclear materials, chemical or biological weapons, or chemical or biological agents; whether in the United States or abroad;
 - b. Fraudulent entry of persons into the United States, the violation of immigration restrictions or the failure to register as a foreign agent or an intelligence trained agent;
 - c. Offenses involving interference with foreign governments or interference with the foreign policy of the United States whether occurring in the United States or abroad;
 - d. Acts of terrorism anywhere in the world which target the U. S. government or its property, U.S. persons, or any property in the United States, or in which the perpetrator is a U.S. person; aircraft hijacking; attacks on aircraft or international aviation facilities; or maritime piracy;
 - e. The unauthorized transportation or use of firearms or explosives in interstate or foreign commerce.
 3. Crimes involving foreign interference with the integrity of U.S. governmental institutions or processes. Such crimes may include:

APPENDIX 9: INTELLIGENCE LAW

SECNAVINST 3820.3E
21 September 2005

- a. Activities to defraud the U.S. government or any federally protected financial institution, whether occurring in the United States or abroad;
 - b. Obstruction of justice or bribery of U.S. officials or witnesses in U.S. proceedings, whether occurring in the United States or abroad;
 - c. Interference with U.S. election proceedings or illegal contributions by foreign persons to U.S. candidates or election committees;
 - d. Perjury in connection with U.S. proceedings, or false statements made in connection with formal reports or applications to the U.S. government, or in connection with a formal criminal or administrative investigation, whether committed in the United States or abroad;
 - e. Counterfeiting U.S. obligations or any other governmental currency, security or identification documents used in the United States, whether committed in the United States or abroad; transactions involving stolen governmental securities or identification documents or stolen or counterfeit non-governmental securities.
4. Crimes related to unauthorized electronic surveillance in the United States or to tampering with, or unauthorized access to, computer systems.
 5. Violations of U.S. drug laws including: the cultivation, production, transportation, importation, sale, or possession (other than possession of user quantities) of controlled substances; the production, transportation, importation, and sale of precursor or essential chemicals.
 6. The transmittal, investment and/or laundering of the proceeds of any of the unlawful activities listed in this Section, whether committed in the United States or abroad.
- B. Any conspiracy or attempt to commit a crime reportable under this section shall be reported if the conspiracy or attempt itself meets the applicable reporting criteria.
- C. The Attorney General also encourages the Agency to notify the Department of Justice when the Agency's otherwise routine collection of intelligence in accordance with its authorities results in its acquisition of information about the commission of other serious felony offenses by non-employees, e.g., violations of U.S. environmental laws relating to ocean and inland water discharging or dumping, drinking water contamination, or hazardous waste disposal, and crimes involving interference with the integrity of U.S. governmental institutions or processes that would not otherwise be reportable under Section VII.A.3.

SECNAVINST 3820.3E
21 September 2005

VIII. Procedures for Submitting Special Crimes Reports

- A. Where the Agency determines that a matter must be the subject of a special report to the Department of Justice, it may, consistent with paragraphs VIII.B and VIII.C, below, make such a report (1) by letter or other, similar communication from the General Counsel, or (2) by electronic or courier dissemination of information from operational or analytic units, provided that in all cases, the subject line and the text of such communication or dissemination clearly reflects that it is a report of possible criminal activity. The Department of Justice shall maintain a record of all special crimes reports received from the Agency.
- B. Where the Agency determines that a matter must be the subject of a special report to the Department of Justice, and where the Agency further determines that no public disclosure of classified information or intelligence sources and methods would result from further investigation or prosecution, and the security of ongoing intelligence operations would not be jeopardized thereby, the Agency will report the matter to the federal investigative agency having jurisdiction over the criminal matter. A copy of that report must also be provided to the AAG, or designated Deputy AAG, Criminal Division.
- C. Where the Agency determines that further investigation or prosecution of a matter that must be specially reported may result in a public disclosure of classified information or intelligence sources or methods or would jeopardize the security of ongoing intelligence operations, the Agency shall report the matter to the AAG or designated Deputy AAG, Criminal Division. A copy of that report must also be provided to the Assistant Director, Criminal Investigations or National Security Divisions, Federal Bureau of Investigation, or in the event that the principal investigative responsibility resides with a different federal investigative agency, to an appropriately cleared person of equivalent position in such agency. The Agency's report should explain the security or operational problems that would or might arise from a criminal investigation or prosecution.
- D. Written documents associated with the reports submitted pursuant to this section may refer to persons who are the subjects of the reports by non-identifying terms (such as "John Doe # _____"). The Agency shall advise the Department of Justice or relevant federal investigative agency of the true identities of such persons if so requested.
- E. It is agreed that, in acting upon information reported in accordance with these procedures, the Agency, the Department of Justice and the relevant federal investigative agencies will deal with classified information, including sources and methods, in a manner consistent with the provisions of relevant statutes and Executive Orders, including the Classified Information Procedures Act.

SECNAVINST 3820.3E

21 September 2005

IX. When Routine Dissemination May be Used in Lieu of A Special Crimes Report

A. Except as set forth in IX.B, below, the Agency may report crimes information regarding non-employees to the Department of Justice by routine dissemination, provided that:

1. the crimes information is of the type that is routinely disseminated by the Agency to headquarters elements of cognizant federal investigative agencies;
2. the criminal activity is of a kind that is normally collected and disseminated to law enforcement by the Agency (e.g., drug trafficking, money laundering, terrorism or sanctions violations); and
3. the persons or entities involved are members of a class that are routinely the targets or objects of such collection and dissemination.

If all three of these conditions are met, the Agency may satisfy its crimes reporting obligation through routine dissemination to the Department of Justice, Criminal Division, and to all cognizant federal law enforcement agencies, which shall retain primary responsibility for review of disseminated information for evidence of criminal activity. In all other cases, the special reporting procedures in Section VIII shall apply. As requested by the Department of Justice, the Agency will coordinate with the Department to facilitate the Department's analytical capabilities as to the Agency's routine dissemination of crimes information in compliance with this MOU.

B. Routine dissemination, as discussed in IX.A, above, may not be used in lieu of the special reporting requirements set forth herein as to the following categories of criminal activities:

1. Certain crimes involving the intentional infliction or threat of death or serious physical harm (VII.A.1, above);
2. Espionage; sabotage; unauthorized disclosure of classified information; and seditious conspiracies to overthrow the government of the United States (VII.A.2.a, above); and
3. Certain crimes involving foreign interference with the integrity of U.S. governmental institutions or processes (VII.A.3.b and c, above).

X. Other Agency Responsibilities

A. The Agency shall develop internal procedures in accordance with the provisions of Sections VIII and IX for the reporting of criminal information by its employees as required under Sections IV.A and VI.A.

B. The Agency shall also establish initial and continuing training to

SECNAVINST 3820.3E
21 September 2005

ensure that its employees engaged in the review and analysis of collected intelligence are knowledgeable of and in compliance with the provisions of this MOU.

XI. Relation to Other Procedures and Agreements

- A. If the Agency desires, for administrative or security reasons, to conduct a more extensive investigation into the activities of an employee relating to any matter reported pursuant to this MOU, it will inform the Department of Justice and the federal investigative agency to which the matter was reported. The Agency may also take appropriate administrative, disciplinary, or other adverse action at any time against any employee whose activities are reported under these procedures. However, such investigations or adverse actions shall be coordinated with the proper investigative or prosecuting officials to avoid prejudice to any criminal investigation or prosecution.
- B. Nothing in these procedures shall be construed to restrict the exchange of information among the Agencies in the Intelligence Community or between those Agencies and law enforcement entities other than the Department of Justice.
- C. This MOU supersedes all prior crimes reporting memoranda of understanding executed pursuant to the requirements of E.O. 12333. To the extent that there exist any conflicts between other Agency policies or directives and the provisions herein, such conflicts shall be resolved in accordance with the provisions of this MOU. However, this MOU shall not be construed to modify in any way the August 1984 Memorandum of Understanding between the Department of Defense and the Department of Justice relating to the investigation and prosecution of certain crimes.
- D. The parties understand and agree that nothing herein shall be construed to alter in any way the current routine dissemination by the Agency of intelligence information, including information regarding alleged criminal activities by any person, to the Department of Justice or to federal law enforcement agencies.

XII. Miscellaneous

- A. This MOU shall become effective as to each agency below as of the date signed by the listed representative of that agency.
- B. The Intelligence-Law Enforcement Policy Board, within one year of the date of the effective date hereof, and as it deems appropriate thereafter, will appoint a working group consisting of an equal number of representatives from the intelligence and law enforcement communities, including the Criminal Division. That working group shall do the following:
 - 1. review the Agency's implementation of Sections III.F and IV.B, hereof;

SECNAVINST 3820.3E
21 September 2005

2. consider whether the crimes reporting requirements of E.O. 12333 and other authorities are being met through the operation of this MOU;
 3. review each of the provisions of this MOU and determine what, if any, modifications thereof should be recommended to the Policy Board, or its successor; and
 4. issue a report to the Policy Board of its findings and recommendations in each of the foregoing categories.
- C. The Policy Board in turn shall make recommendations to the Attorney General, the Director of Central Intelligence, and the heads of the affected agencies concerning any modifications to the MOU that it considers necessary.

Janet Reno
Attorney General
Date: August 3, 1995

William J. Perry
Secretary of Defense
Date: 11 AUG 1995

John Deutch
Director of Central
Intelligence
Date: 3 August 1995

James M. McConnell
Director, National Security Agency
Date: 22 AUG 95

Michael J. Munson
Director, Defense
Intelligence Agency
Date: 2 Aug 95

Toby T. Gab
Assistant Secretary of State,
Intelligence and Research
Date: 8/14/95

Kenneth E. Baker
Director, Office Of Non-Proliferation and National Security,
Department of Energy
Date: 15 Aug 95

**Appendix 9-6: SECNAVINST 3850.2C – Dep’t of the Navy
Counterintelligence**

APPENDIX 9: INTELLIGENCE LAW

DEPARTMENT OF THE NAVY
OFFICE OF THE
SECRETARY 1000 NAVY
PENTAGON WASHINGTON,
DC 20350-1000

SECNAVINST 3850.2C
N2E 20 Jul 2005

SECNAV INSTRUCTION 3850.2C

From: Secretary of the Navy To: All Ships and Stations Subj:

DEPARTMENT OF THE NAVY COUNTERINTELLIGENCE Ref: (a)

DOD Directive 5240.2 of 22 May 97

(b) DOD 5240.6 of 09 Aug 04

I

(c) Executive Order 12333

(d) DO Instruction 5240.1R

D

(e) Counterintelligence Enhancement Act of 2002
107-306, Title 14, No 27, 2002)

(Pub.L.

1. Purpose: To implement references (a) and (b), delineate responsibilities for counterintelligence (CI) within the Department of the Navy (DON), ensure DON CI activities are conducted in a coordinated manner and pursuant to references (a) through (g). This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation: SECNAVINST 3850.2B and SECNAVINST 3875.1A

3. Background: CI is critical to the protection of Navy and Marine Corps forces, operations, information, facilities, equipment and networks from attack and the intelligence activities of foreign governments and international terrorist organizations. Department of Defense (DOD) policy directs CI activities shall be conducted in a comprehensive, integrated and coordinated effort within the department and also integrated into the national CI structure pursuant to reference (e).

4. Definitions

a. Counterintelligence: Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, foreign persons or international terrorist organizations.

Appendix 9-7: Policy Guidance for Intel Support in CONUS

UNCLASSIFIED



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, DC 20310-1001



DAMI-CHI (100)

19 Feb 99

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Policy Guidance for Intelligence Support to Force Protection in CONUS

1. References:

- a. AR 381 -10, U.S. Army Intelligence Activities, 1 Aug 84.
- b. AR 381-12, Subversion and Espionage Directed Against the Army (SAEDA) 15 Jan 93.
- c. AR 381-20, The Army Counterintelligence Program, 15 Nov 93.
- d. AR 525-13, Antiterrorism Force Protection (AT/FP): Security of Personnel, Information, and Critical Resources, 10 Sep 98.
- e. DoD message, ATSD-10, dtg 181700Z Nov 98, subject: Policy Guidance for Intelligence Support to Force Protection (enclosed).

2. Reference 1a governs Military Intelligence (MI) activities that affect United States Persons, and states that authority to employ certain collection techniques is limited to that necessary to perform functions assigned to the intelligence component. References 1b-1d assign more specific functions and responsibilities for intelligence support to force protection. Reference 1e is the most current DoD guidance.

3. This memo implements reference 1e and provides additional guidance:

a. Although reference 1e refers to a DoD list of U.S. Persons and organizations against whom DoD intelligence elements may collect, Army MI elements may not conduct intelligence activities specifically targeting them. Because the Army maintains its law enforcement separately from its intelligence elements, it is inappropriate to collect information on these persons and organizations through intelligence activities. The Army designated law enforcement as the responsible agency, per reference 1d.

b. MI elements will no longer report U.S. criminal threat information as intelligence or SAEDA incident reports. This change is being included in the revision of references 1b and 1c. Note that this does not pertain to national security crimes (treason, spying, espionage, sedition, subversion, etc.) which are within MI responsibility per reference 1c.

UNCLASSIFIED

UNCLASSIFIED

DAMI-CHI

SUBJECT: Policy Guidance for Intelligence Support to Force Protection in CONUS

c. MI personnel will pass, via the most expedient method, U.S. criminal and U.S. terrorist threat information received through normal assigned activities ("incidentally acquired") to the Provost Marshal/Director of Security and the U.S. Army Criminal Investigation Command (USACIDC). Receiving and passing the information fully complies with references 1a and 1e. Do not send copies to the HQDA Antiterrorism Operations and Intelligence Cell or Army Counterintelligence Center, as it could create circular reporting or false confirmation. USACIDC has that reporting responsibility, per reference 1d. A synopsis may be filed in general correspondence files ("administrative purposes"), as needed, for crediting work done.

d. MI personnel will refer requests for U.S. terrorist and U.S. criminal threat information and assessments to USACIDC or the Provost Marshal, in accordance with reference 1d. Local threat assessments are the installation's responsibility; MI may augment the local information with foreign intelligence and counterintelligence information and analysis.

e. MI personnel participating in AT/FP assessment teams per reference 1d are responsible for foreign intelligence and counterintelligence information and analysis. They may provide analytical advice and assistance to other team personnel in developing the overall assessment, but should not be used as the analytical subject matter expert for non-MI functional areas.

f. Any MI element may request a collectability determination through command channels to HQDA (DAMI-CHI), in accordance with references 1a and 1e. Because of the 90-day retention time limit in reference 1a, commanders must ensure speedy transmittal to HQDA.

4. This memo was coordinated with the Office of the Army General Counsel, Office of The Judge Advocate General, Office of The Inspector General, Office of the Deputy Chief of Staff for Operations, USACIDC, and the Intelligence and Security Command.

5. Ensure widest possible dissemination to commanders, operations personnel, installation security officials, provosts marshal, inspectors general, criminal investigative and intelligence elements. MACOM supplements require HQDA prior approval.

End

Original Signed
CLAUDIA J. KENNEDY
Lieutenant General, GS
Deputy Chief of Staff
for Intelligence

2
UNCLASSIFIED

UNCLASSIFIED

DAMI-CHI

SUBJECT: Policy Guidance for Intelligence Support to Force Protection in CONUS

DISTRIBUTION:

U.S. Army Corps of Engineers
U.S. Army Criminal Investigation Command
U.S. Army Forces Command
U.S. Army Intelligence and Security Command
U.S. Army Materiel Command
U.S. Army Medical Command
U.S. Military Academy
U.S. Army Military District of Washington
Military Traffic Management Command
National Guard Bureau
U.S. Army Pacific
U.S. Army Reserve Command
U.S. Army Space and Missile Defense Command
U.S. Army Special Operations Command
Third U.S. Army
U.S. Army Training and Doctrine Command
U.S. Army Intelligence Center and Fort Huachuca

CF:

ATSD-10
SAGC
SAIG-10
DAJA-10
DAMO-ODL
Eighth U.S. Army
U.S. Army Europe and Seventh Army
U.S. Army South
650th Military Intelligence Group

³
UNCLASSIFIED

UNCLASSIFIED

UUUUU

P 181700Z NOV 98

FM SECDEF WASHINGTON DC//ATSD-IO//

TO RUEKJCS//JOINT STAFF WASHINGTON DC//OJCS-LA/DJS//IG/J2/J3//

RUEADWD//SECARMY WASHINGTON DC//SAIG-IO/GC//

RUEAAAA//SECNAV WASHINGTON DC//NAVINSGEN/GC//

RUEAHQA//OSAF WASHINGTON DC//SAF-IG//GC//

RUEADWD//CSA WASHINGTON DC//DACS/DAM//DAJA/DAMO/DAAR//

RUEAAAA//CNO WASHINGTON DC//N00/N09/N095/N2/N3/N5/NLSC//

RUEAHQA//CSAF WASHINGTON DC//CC/CV/XO/XO//JAG/AF-RE//

RUEACMC//CMC WASHINGTON DC//CMC/ACMC//G/SJA/CL/C4//PP&O/MCRC//

RUFGNOA//USCINCEUR VA//HINGEN GE//IG/J2/J3/SJA//

RULYSCC//USACOM NORFOLK VA//IG/J2/J3/SJA//

RUCJACC//USCINCCENT MACDILL AFB FL//IG/J2/J3/SJA//

RUCJAAA//USSOCOM MACDILL AFB FL//IG/J2/J3/SJA//CORB//

RUMIAAA//USCINCSO MIAMI FL//IG/J2/J3/SJA//

RUPEUNA//USCINCSpace PETERSON AFB CO//IG/J2/J3/SJA//

RHCJAAA//USCINCTRANS SCOTT AFB IL//IG/J2/J3/SJA//

RHHMUNA//USCINCPAC HONOLULU HI//IG/J2/J3/SJA//

RUCJSTR//USCINCSSTRAT OFFUTT AFB NE//IG/J2/J3/SJA//

RUJETIAA//DIRNSA FT GEORGE G MEADE MD//IG/GC/NSOC//

PAGE 02 RUEKJCS8619 UNCLAS

RUEKDIA//DIA WASHINGTON DC//IG/J2/GC/DO/DHS/DAC/DAJ/DIO/MC//

RUEBMJB//NRO WASHINGTON DC//IG/GC//

RUEALIU//NIMA WASHINGTON DC//IG/GC//

RUEAADN//DTRA WASHINGTON DC//IG/GC/C//

RUEAUSA//CNGB WASHINGTON DC//NGC-ZA//NCG-ARZ//NGB-IG//

RUEAUSA//NGB WASHINGTON DC//CF//

INFO RUEKJCS//SECDEF WASHINGTON DC//GC/IG/USDP/C3//ATSD-IO//

RUDHAAA//CDRINSCOM FT BELVOIR VA//CDR/CS-IO//IG/DCSOPS/SJA//

RUCXNLG//ONI SUITLAND MD//IG/GC//

RUDHNIS//DIRNAVCRIMINVSERV WASHINGTON DC//IG/GC//

RUQVAIA//AIA KELLY AFB TX//CC/CV//IG/INSJA//

RUEDADI//AFOSI BOLLING AFB DC//CC/CV//IG/SJA//

RUWMBFA//AFIA KIRTLAND AFB NM//CC/IG-IO//

RULSMCA//MCIA QUANTICO VA

BT

UNCLAS SUBJECT: POLICY GUIDANCE FOR INTELLIGENCE SUPPORT TO FORCE PROTECTION

REFERENCES:

A. EXECUTIVE ORDER 12333

PAGE 03 RUEKJCS8619 UNCLAS

B. DODD 5240.1

C. DODD 5200.27

D. DOD REG 5240.1-R

E. MCM 75-91

F. AR 381-10

G. SECNAVINST 3820.3D

H. AFI 14-104

J. MCO 3800.2A

J. DIRECTOR OF COUNTERINTELLIGENCE MEMO, "AUTHORITY TO COLLECT INFORMATION ON DOMESTIC TERRORIST AND OTHER GROUPS COMMITTING ILLEGAL ACTS THAT POSE A THREAT TO THE DEPARTMENT OF DEFENSE (U)," DATED 27 JAN 98.

UNCLASSIFIED

UNCLASSIFIED

1. THE PURPOSE OF THIS MESSAGE IS TO PROVIDE POLICY GUIDANCE TO COMMANDERS AND SUPPORTING DOD INTELLIGENCE ORGANIZATIONS REGARDING PERMISSIBLE INTELLIGENCE SUPPORT FOR FORCE PROTECTION ACTIVITIES.
2. THIS MESSAGE HAS BEEN COORDINATED WITH THE JOINT STAFF; THE DOD GENERAL COUNSEL; THE INSPECTOR GENERAL, DOD; THE UNDERSECRETARY OF DEFENSE FOR POLICY; AND THE SENIOR CIVILIAN OFFICIAL IN THE OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE.

PAGE 04 RUEKJCS8619 UNCLAS

3. FORCE PROTECTION IS A FUNDAMENTAL COMMAND RESPONSIBILITY FOR ALL COMMANDERS WHEREVER LOCATED. DOD INTELLIGENCE AND COUNTERINTELLIGENCE (INTEL/CI) COMPONENTS HAVE AN IMPORTANT ROLE TO PLAY IN SUPPORT OF THE COMMANDERS' FORCE PROTECTION MISSION. EXECUTIVE ORDER 12333 AND DOD 5240.1-R REGULATE THE CONDUCT OF INTEL/CI ACTIVITIES; THE ATTORNEY GENERAL HAS APPROVED THE PROCEDURES IN DOD 5240.1-R. THEIR PURPOSE IS TO ENABLE DOD INTEL/CI COMPONENTS TO CARRY OUT EFFECTIVELY THEIR AUTHORIZED FUNCTIONS WHILE ENSURING THAT THEIR ACTIVITIES THAT AFFECT UNITED STATES PERSONS ARE CARRIED OUT IN A MANNER THAT PROTECTS THE CONSTITUTIONAL RIGHTS AND PRIVACY OF SUCH PERSONS.
4. INTEL/CI COMPONENTS DO NOT HAVE A LAW ENFORCEMENT MISSION. LAW ENFORCEMENT IS THE RESPONSIBILITY OF THOSE AGENCIES SPECIFICALLY CHARTERED TO HANDLE LAW ENFORCEMENT MATTERS, E.G., PROVOST MARSHAL; CID; OSI; AND NCIS. (NOTE: AFOSI AND NCIS HAVE BOTH COUNTERINTELLIGENCE AND LAW ENFORCEMENT MISSIONS, WHICH ARE MANAGED SEPARATELY WITHIN THESE ORGANIZATIONS.) OFF THE INSTALLATION IN CONUS, LAW ENFORCEMENT IS THE RESPONSIBILITY OF LOCAL AND STATE LAW ENFORCEMENT OFFICIALS AND THE FBI AT THE FEDERAL LEVEL, NOT DOD INTEL/CI COMPONENTS.
5. WHEN FOREIGN GROUPS OR PERSONS THREATEN DOD PERSONNEL, RESOURCES,

PAGE 05 RUEKJCS8619 UNCLAS

- OR ACTIVITIES – WHETHER CONUS OR OCONUS – DOD INTEL/CI COMPONENTS MAY INTENTIONALLY TARGET, COLLECT, RETAIN, AND DISSEMINATE INFORMATION ON THEM (UNLESS THE GROUPS OR PERSONS IN QUESTION MEET THE DEFINITION OF UNITED STATES PERSONS IN EXECUTIVE ORDER 12333/DOD 5240.1-R – SEE PARA 11A BELOW). BOTH CONUS AND OCONUS, INTEL/CI COMPONENTS ARE RESTRICTED IN WHAT AND HOW THEY CAN COLLECT, RETAIN, AND DISSEMINATE INFORMATION WITH RESPECT TO UNITED STATES PERSONS, AS EXPLAINED BELOW.
6. COMMANDERS MAY NOT LEGALLY DIRECT DOD INTEL/CI COMPONENTS TO TARGET OR INTENTIONALLY COLLECT INFORMATION FOR FORCE PROTECTION PURPOSES ON U.S. PERSONS UNLESS SUCH PERSONS HAVE BEEN IDENTIFIED IN REFERENCE J, OR SUBSEQUENT VERSIONS. THE FBI PARTICIPATES IN THE IDENTIFICATION OF THESE PERSONS.
7. COMMANDERS SHOULD BE COGNIZANT, HOWEVER, OF THE FACT THAT DURING THE CONDUCT OF ROUTINE LIAISON ACTIVITIES, DOD INTEL/CI COMPONENTS OFTEN RECEIVE INFORMATION IDENTIFYING U.S. PERSONS ALLEGED TO THREATEN DOD RESOURCES, INSTALLATIONS, MATERIEL, PERSONNEL, INFORMATION, OR ACTIVITIES. DOD INTEL/CI ACTIVITIES MAY ACT AS A CONDUIT AND MUST PASS ANY THREAT INFORMATION INCIDENTALLY RECEIVED IN THIS MANNER TO THE THREATENED COMMANDER AND THE ENTITY WHICH HAS

PAGE 06 RUEKJCS8619 UNCLAS

- RESPONSIBILITY FOR COUNTERING THAT THREAT (E.G., MILITARY POLICY, PROVOST MARSHAL, OR SECURITY DIRECTOR). THIS TRANSMITTAL OF INFORMATION DOES NOT CONSTITUTE COLLECTION BY THE DOD INTEL/CI ORGANIZATION WITHIN THE MEANING OF DOD REGULATION 5240.1-R (REFERENCE D), AND IS THEREFORE PERMISSIBLE. HOWEVER, ANY FOLLOW-ON INTEL/CI INVESTIGATION, COLLECTION, OR TARGETING OF SUCH U.S.

UNCLASSIFIED

UNCLASSIFIED

PERSONS WOULD BE SUBJECT TO EXISTING PROCEDURES AS SET FORTH IN REFERENCES A THROUGH J.

8. LAW REFERENCE C., DOD LAW ENFORCEMENT AND SECURITY ORGANIZATIONS – AS OPPOSED TO INTEL/CI COMPONENTS – MAY LEGALLY ACCEPT AND RETAIN FOR UP TO 90 DAYS, UNLESS LONGER RETENTION IS REQUIRED BY LAW OR PERMISSION IS SPECIFICALLY GRANTED BY THE SECRETARY OF DEFENSE OR HIS DESIGNEE INFORMATION PERTAINING TO U.S. PERSONS WHICH THREATENS DOD RESOURCES, PERSONNEL, INSTALLATIONS, MATERIEL, INFORMATION, OR ACTIVITIES. COMMANDERS SHOULD TAKE APPROPRIATE ADVANTAGE OF LAW ENFORCEMENT LIAISON ACTIVITIES TO MONITOR CRIMINAL ACTIVITY IN THE VICINITY OF THEIR INSTALLATIONS/ACTIVITIES (ACTS OF TERROR, ASSAULT, THREATS OF HARM, OR DESTRUCTION OF GOVERNMENT PROPERTY ARE CRIMINAL ACTS).
9. TO CLARIFY THE ROLE OF DOD INTEL/CI ORGANIZATIONS IN SUPPORTING

PAGE 07 RUEKJCS8619 UNCLAS

COMMANDERS' FORCE PROTECTION RESPONSIBILITIES, THE FOLLOWING GUIDANCE IS EFFECTIVE ON RECEIPT.

- A. WHEN DOD INTEL/CI ORGANIZATIONS LEARN OF INFORMATION PRESENTING A REASONABLE BELIEF THAT A U.S. PERSON OTHER THAN A PERSON IDENTIFIED BY THE DOD DIRECTOR OF COUNTERINTELLIGENCE (IN REFERENCE J) POSES A THREAT TO DEPARTMENTAL RESOURCES, PERSONNEL, INSTALLATIONS, MATERIEL, INFORMATION, OR ACTIVITIES, THE ACQUIRING UNIT SHALL IMMEDIATELY ALERT THE APPROPRIATE OFFICIAL OF THE THREATENED ENTITY AND PROVIDE THE INFORMATION TO THE APPROPRIATE LAW ENFORCEMENT AUTHORITY. FOLLOWING SUCH NOTIFICATION, IF THE ACQUIRING UNIT HAS REASON TO PERMANENTLY RETAIN THAT INFORMATION UNDER THE PROVISION OF PROCEDURE 3 OF DOD REGULATION 5240.1-R, IT SHALL REQUEST, BY THE MOST EXPEDITIOUS MEANS AVAILABLE AND THROUGH ITS SERVICE INTELLIGENCE COMPONENT, THAT OASD(C3I) EVALUATE THE ACQUIRED INFORMATION FOR RETENTION ("COLLECTABILITY DETERMINATION"). OASD(C3I) WILL COORDINATE THE REQUEST WITH THE DOD GENERAL COUNSEL AND THE ATSD(IO) PRIOR TO NOTIFYING THE SERVICE INTELLIGENCE COMPONENT OF APPROVAL/DISAPPROVAL OF THE REQUEST. THE MILITARY SERVICES ARE ENJOINED TO PROCESS COLLECTABILITY DETERMINATIONS EXPEDITIOUSLY.
- B. WHILE AWAITING A COLLECTABILITY/RETAINABILITY DETERMINATION, THE ACQUIRING UNIT MAY INDEX THE INFORMATION AND MAINTAIN IT ON FILE FOR A 90 DAY PERIOD. IF, DURING THAT 90 DAY PERIOD, THE ACQUIRING UNIT LEARNS OF ADDITIONAL INFORMATION RELATING TO THE THREAT POSED BY THE U.S. PERSON IN

PAGE 03 RUEKJCS8619 UNCLAS

QUESTION, THE UNIT SHALL IMMEDIATELY PASS THAT INFORMATION TO THE APPROPRIATE OFFICIAL OR LAW ENFORCEMENT AUTHORITY. (THIS INFORMATION MAY BE DISSEMINATED TO AFFECTED COMMANDERS AND SECURITY OFFICIALS, ONLY.)

- C. IF OASD(C3I) DENIES PERMISSION TO COLLECT OR RETAIN INFORMATION ON THE U.S. PERSON, THE REQUESTING ORGANIZATION WILL REMOVE ALL INFORMATION PERTAINING TO THAT U.S. PERSON FROM ITS FILES AND DESTROY IT OR TRANSFER IT TO A DOD LAW ENFORCEMENT OR SECURITY ACTIVITY WHICH HAS AN OFFICIAL NEED FOR THE INFORMATION. OASD(C3I) WILL PROVIDE TO OATSD(IO) AND THE GENERAL COUNSEL, WITHIN FIVE WORKING DAYS, ONE COPY OF ALL PERMISSIONS TO COLLECT/RETAIN INFORMATION ON U.S. PERSONS NOT LISTED IN REFERENCE J. WITHIN 30 DAYS OF RECEIPT OF THIS MESSAGE, HEADS OF DOD INTEL/CI COMPONENTS WILL PROVIDE TO OATSD(IO) ONE COPY OF ANY INSTRUCTIONS ISSUED WHICH IMPLEMENT THIS MESSAGE.

10. REQUEST HEADS OF DOD INTEL/CI COMPONENTS ENSURE THAT ALL FIELD LOCATIONS PROVIDING INTELLIGENCE SUPPORT TO COMMANDERS RECEIVE A COPY OF THIS MESSAGE.
11. ADDRESSEES ARE INVITED TO VISIT OUR RECENTLY ACTIVATED ATSD(IO) HOMEPAGE ON THE INTERNET AT WWW.DTIC.MIL/ATSDIO.

PAGE 04 RUEKJCS8619 UNCLAS

12. DEFINITIONS:

UNCLASSIFIED

UNCLASSIFIED

A. FROM APPENDIX A, DOD REGULATION 5240.1-R:

(1) THE TERM "U.S. PERSONS" MEANS:

(A) A U.S. CITIZAN;

(B) AN ALIEN KNOWN BY THE DOD INTELLIGENCE COMPONENT CONCERNED TO BE A PERMANENT RESIDENT ALIEN (PRA);

(C) AN UNINCORPORATED ASSOCIATION SUBSTANTIALLY COMPOSED OF U.S. CITIZENS OR PRAS;

(D) A CORPORATION INCORPORATED IN THE U.S., 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 U.S., IS NOT A U.S. PERSON.

[A PERSON OR ORGANIZATION OUTSIDE THE U.S. SHALL BE PRESUMED NOT TO BE A U.S. PERSON UNLESS SPECIFIC INFORMATION TO THE CONTRARY IS OBTAINED. AN ALIEN IN THE U.S. SHALL BE PRESUMED NOT TO BE A U.S. PERSON UNLESS SPECIFIC INFORMATION TO THE CONTRARY IS OBTAINED.]

[A PERMANENT RESIDENT ALIEN IS A FOREIGN NATIONAL LAWFULLY ADMITTED INTO THE U.S. FOR PERMANENT RESIDENCE AND,

PAGE 05 RUEKJCS8619 UNCLAS

THEREFORE, IS A U.S. PERSON.]

(2) FOREIGN INTELLIGENCE IS INFORMATION RELATING TO THE CAPABILITIES, INTENTIONS, AND ACTIVITIES OF FOREIGN POWERS, CAPABILITIES, INTENTIONS, AND ACTIVITIES OF FOREIGN POWERS, ORGANIZATIONS, OR PERSONS, BUT NOT INCLUDING COUNTERINTELLIGENCE EXCEPT FOR INFORMATION ON INTERNATIONAL TERRORIST ACTIVITIES.

(3) COUNTERINTELLIGENCE IS 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.

B. FROM JOINT PUB 2-01, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS, DATED 23 MAR 94: FORCE PROTECTION IS DEFINED AS "SECURITY PROGRAM DESIGNED TO PROTECT SOLDIERS, CIVILIAN EMPLOYEES, FAMILY MEMBERS, FACILITIES, AND EQUIPMENT, IN ALL LOCATIONS AND SITUATIONS, ACCOMPLISHED THROUGH PLANNED AND INTEGRATED APPLICATION OF COMBATING TERRORISM, PHYSICAL SECURITY, OPERATIONS SECURITY, PERSONAL PROTECTIVE SERVICES, AND SUPPORTED BY INTELLIGENCE, COUNTERINTELLIGENCE, AND OTHER SECURITY PROGRAMS."

UNCLASSIFIED