



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

SECNAVINST 3850.2E
DUSN (P)
January 3, 2017

SECNAV INSTRUCTION 3850.2E

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY COUNTERINTELLIGENCE

Ref: See enclosure (1)

Encl: (1) References
(2) Definitions
(3) Responsibilities

1. Purpose. This instruction provides policy and defines specific responsibilities for Counterintelligence (CI) in the Department of the Navy (DON), per references (a) through (ag). This instruction has been revised and should be read in its entirety.

2. Cancellation. SECNAVINST 3850.2D

3. Definitions. See enclosure (2).

4. Applicability. This instruction applies to the Office of the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and all DON CI activities, components, and personnel including supporting contractors and consultants engaged in the management, oversight or execution of CI activities for or on behalf of the DON.

5. Policy. It is DON policy that:

a. The DON and its components shall integrate CI activities into all operations, programs, systems, exercises, plans, doctrine, strategies, policies, and architectures to detect, identify, assess, exploit, and deny Foreign Intelligence Entities (FIE) and their insiders targeting or exploiting DON information, personnel,

3 Jan 17

operations and other activities per references (a) through (g).

b. DON CI activities shall be integrated into the national CI structure and be conducted in a comprehensive, integrated, and coordinated effort per reference (a).

c. DON CI activities shall be integrated into all operations, programs, systems, exercises, plans, doctrine, strategies, policies, and architectures for the protection of U.S. Navy (USN) and U.S. Marine Corps (USMC) forces and infrastructure per reference (b).

d. DON CI personnel conducting CI activities, must successfully complete formal CI training approved by the Under Secretary of Defense for Intelligence (USD(I)), the Secretaries of the Military Departments, or the Director, Defense Intelligence Agency (DIA), per reference (a).

e. The Naval Criminal Investigative Service (NCIS) is the DON lead agency for the conduct of Offensive CI Operations (OFCO) per references (a), (b), and (h). DON OFCO shall be conducted as a coordinated activity from combined operating locations.

f. The Under Secretary of the Navy (UNSECNAV) oversees all DON CI activities and shall be supported in these duties by the General Counsel of the Navy (GC) and Deputy Under Secretary of the Navy for Policy (DUSN (P)) per references (i), (j), and (k).

g. The NCIS is the only DON component authorized to conduct CI investigations per references (a), (b), and (c).

h. The NCIS serves as the coordinating authority of all DON CI activities and will respond to Service inquiries in a timely manner per references (a), (b), (d), (e), (h), and (l), of this instruction. Coordination and disagreement resolution within the DON shall be continuous and at the lowest possible level throughout the course of all CI activities.

3 Jan 17

i. When not operating under the authorities of a Geographic Combatant Commander (GCC) or a non-DON intelligence element, DON components shall coordinate and de-conflict the conduct of CI activities in the United States, its territories, and overseas. Coordination and de-confliction shall be conducted at the earliest opportunity, but shall not impede the execution of time-sensitive CI activities.

j. All DON CI activities which involve the use of clandestine methods shall be conducted per references (d), (e), (f), and (i).

k. DON CI personnel, when assigned to a GCC, shall conduct CI activities under their authority, direction, and control.

l. DON CI personnel, as defined in enclosure (2) of this instruction, may conduct CI activities as follows:

(1) When assigned or detailed to NCIS, CI personnel shall conduct CI activities under the authority, direction, and control of the Director, NCIS (DIRNCIS).

(2) In all other cases, when properly coordinated and de-conflicted, CI personnel may conduct authorized CI activities on behalf of the command to which they are assigned under the authority, direction, and control of Director of Naval Intelligence (DNI) or Director of Intelligence (DIRINT), Headquarters Marine Corps. Activities include:

(a) CI Analysis and Production, per references (d) and (m).

(b) OFCO, per reference (e).

(c) CI Collection, per reference (n).

(d) CI Functional Services, per references (a) and (o).

3 Jan 17

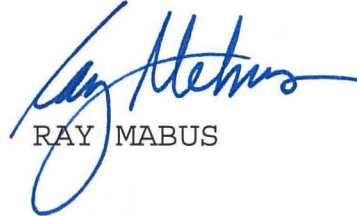
(e) Support to NCIS CI Investigations, per reference (b).

(f) Liaison with U.S. and foreign government officials following coordination with the appropriate GCC and U.S. country team, per reference (e).

6. Responsibilities. See enclosure (3).

7. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per reference (p).

8. Forms and Reports. The reporting requirements contained in enclosure (3), paragraphs 3, 4, and 5 are exempt from reports control per SECNAV M-5214.1 of December 2005, Part IV, paragraphs 7g, 7i, 7n, and 7o.



RAY MABUS

Distribution:

Electronic only, via Department of the Navy Issuances Web site <http://doni.documentservices.dla.mil/>

3 Jan 17

REFERENCES

- (a) DoD Directive O-5240.02 of 17 March 2015
- (b) DoD Instruction 5240.04 of 2 February 2009,
Incorporating Change 1, 15 October 2013
- (c) DoD Instruction O-5240.21 of 14 May 2010,
Incorporating Change 2, 15 October 2013
- (d) SECNAVINST 5430.107
- (e) DoD Instruction S-5240.09A of 2 February 2015
- (f) Counter Intelligence Enhancement Act of 2002, Pub. L.
107-306, Title IX, §901(a), 27 November 2002, 116
Stat. 2432, 50 USC §3001 note.
- (g) DoD Directive 5240.06 of 17 May 2011, Incorporating
Change 1, 30 May 2013
- (h) E.O. 12333 as amended 30 July 2008
- (i) DoD Instruction 5240.26 of 4 May 2012, Incorporating
Change 1, 15 October 2013
- (j) SECNAVINST 5430.7Q
- (k) DoD Instruction 5240.10 of 5 October 2011,
Incorporating Change 1, 15 October 2013
- (l) DoD Instruction 5200.30 of 28 May 2015
- (m) DoD Instruction 5240.18 of 17 November 2009,
Incorporating Change 1, 15 October 2013
- (n) DoD Instruction S-5240.17 of 14 March 2014
- (o) DoD Instruction 5240.16 of 27 August 2012,
Incorporating Change 1, 15 October 2013
- (p) SECNAVINST M-5210.1
- (q) JP 1-02, 12 April 2001 as amended April 2010
- (r) DoD Directive 5210.48 of 24 April 2015
- (s) DoD Instruction 5240.25 of 30 March 2012,
Incorporating Change 1, 15 October 2013
- (t) DoD Instruction S-5240.23 of 13 December 2010,
Incorporating Change 1, 16 October 2013
- (u) DoD Instruction 5240.05 of 3 April 2014
- (v) SECNAVINST 3850.4A
- (w) SECNAVINST 5500.30F
- (x) SECNAVINST 3820.3E
- (y) DoD Directive 5143.01 of 24 October 2014,
Incorporating Change 1, 22 April 2015
- (z) E.O. 13587
- (aa) SECNAVINST 5510.30B
- (ab) DoD Instruction O-5240.24 of 8 June 2011,
Incorporating Change 1, 15 October 2013

3 Jan 17

- (ac) DoD Directive S-3325.09 of 9 January 2014,
Incorporating Change 2, 15 July 2014
- (ad) DoD Instruction 5240.1-R of December 1982
- (ae) MOA between NCIS and DNI of 6 Oct 2014
- (af) SECNAVINST 5000.34E
- (ag) JP 2-01.02, 16 March 2011

3 Jan 17

DEFINITIONS

1. Coordinating Authority. For the purpose of this instruction, the authority delegated to an organization or individual for coordinating specific functions and activities involving forces of two or more military services, or two or more forces of the same department. The organization or individual has the authority to require consultation between the forces involved, but does not have the authority to compel agreement.

2. Coordination. For the purposes of this instruction, coordination is defined as a prerequisite to de-confliction; advising of intent, sharing details of execution, ensuring mutual support, and providing after-action information.

3. Counterintelligence. Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, assassinations conducted for or on behalf of foreign powers, organizations, persons, or their agents, or international terrorist organizations or activities.

4. Counterintelligence Activities. One or more of the CI functions of analysis, collection, functional services, investigations, operations, and production.

5. Counterintelligence Analysis and Production Element. The element within a Defense CI Component that performs CI analysis in any form; produces a CI analytical product in any of the categories of CI analysis; or responds to requests for CI analysis from an internal organization and/or from organizations external to the Defense CI Component, per reference (m).

6. Counterintelligence Collection. The systematic acquisition of intelligence information to answer CI collection requirements.

3 Jan 17

7. Counterintelligence Functional Services. CI activities conducted to support the four missions of CI and that enable one or more of the other functions.

8. Counterintelligence Inquiry. An examination of facts surrounding an incident of potential CI interest to determine if a CI investigation is necessary, per references (a) and (b).

9. Counterintelligence Insider Threat. A person, known or suspected, who uses their authorized access to DoD facilities, personnel, systems, equipment, information, or infrastructure to damage and disrupt operations, compromise DoD information, or commit espionage on behalf of a FIE.

10. Counterintelligence Investigations. Formal investigative activities undertaken to determine whether a particular person is acting for or on behalf of, or an event is related to, a foreign power engaged in spying, or committing espionage, sabotage, treason, sedition, subversion, assassinations, or international terrorist activities, and to determine actions required to neutralize such acts.

11. Counterintelligence Operations. Proactive activities designed to identify, deceive, exploit, disrupt, neutralize, or deter FIE activities.

12. Counterintelligence Personnel. For the purposes of this instruction, CI personnel are defined as members of the DON, to include reserve personnel, that have successfully completed formal CI training approved by USD(I), the Secretaries of the Military Departments, or the Director, DIA and are assigned in a billet with the authority to conduct authorized CI activities.

13. Counterintelligence Production. The process of analyzing all-source information concerning espionage or other multidiscipline intelligence collection threats, sabotage, terrorism, and other related threats to U.S. military commanders, the DoD, and the U.S. Intelligence Community (IC) and developing it into a final product that is disseminated per reference (q).

3 Jan 17

14. De-confliction. For the purpose of this instruction, the process of sharing information regarding collection between multiple agencies to eliminate potential duplication of effort, multiple unintended use of the same source, or circular reporting.

15. Foreign Intelligence Entity. Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupts U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists.

16. Lead Agency. For the purpose of this instruction, the organization designated to coordinate the inter-departmental oversight of ongoing CI activities.

17. Military Department Counterintelligence Organization (MDCO). A CI element, within a Military Department, that is authorized to conduct CI Investigations. The MDCOs are Army CI, NCIS, and the Air Force Office of Special Investigations.

18. Offensive Counterintelligence Operation. A clandestine CI activity conducted for military, strategic, DoD, or national CI and security purposes against a target having suspected or known affiliation with FIEs, international terrorism, or other foreign persons or organizations, to counter terrorism, espionage, or other clandestine intelligence activities that threaten the security of the Department or the U.S. The two types of OFCO are double agent operation and controlled source operation.

3 Jan 17

RESPONSIBILITIES

1. The SECNAV is responsible for and maintains oversight authority over all DON CI activities.
2. The UNSECNAV shall:
 - a. Exercise oversight of all DON CI activities per references (d), (f), and (h).
 - b. Serve as the approving authority for all OFCO operational proposals.
 - c. Promptly and fully inform SECNAV regarding any action taken involving or affecting the DON, as well as any significant and/or sensitive CI activity, questionable CI activity, and intelligence-related activities.
3. DUSN (P) shall:
 - a. Ensure coordination and execution across the DON and assist the UNSECNAV with oversight responsibilities.
 - b. Monitor and oversee CI activities, programs, and resources to ensure compliance with national, DoD, and DON CI policies.
 - c. Manage and coordinate strategic CI matters.
 - d. Coordinate with the DIRNCIS, DNI, and DIRINT on the DON position for those forums and groups with USN and USMC CI interests that only allow one voting representative per department.
4. The DIRNCIS shall:
 - a. Be the principal advisor to the DON Secretariat for CI matters.
 - b. Serve as the Coordinating Authority for all DON CI activities.

3 Jan 17

- c. As the DON lead agency for the conduct of OFCO, ensure USN, USMC, and NCIS OFCO are coordinated and responsibilities are per reference (e).
- d. Be designated as the DON MDCO representative.
- e. Ensure NCIS CI requirements and responsibilities are identified, documented, and reported to the UNSECNAV, GC, DUSN (P), Naval Inspector General (NAVINSGEN), Inspector General of the Marine Corps (IGMC), and Senior Review Board (SRB) on an annual basis and as required.
- f. Exercise authority, direction, and control over NCIS CI personnel and activities.
- g. Conduct full-spectrum CI activities, to include CI investigations, in support of the DON and its components.
- h. Ensure NCIS initiates, conducts, and directs CI, terrorism and related investigations designed to identify, detect, or neutralize espionage or terrorist planning and activities regardless of command authorization per references (a), (b), (c), and (d).
- i. Ensure CI requirements beyond NCIS capacity or authority to address are identified and presented to the UNSECNAV, GC, and DUSN (P) for resolution.
- j. Provide quarterly CI budget and resource execution reports to the DNI.
- k. Organize, train, and equip NCIS CI personnel per reference (a).
- l. In coordination with DNI and DIRINT, maintain a database of all issued CI credentials per references (f), (g), (l), (r), and (s).
- m. Establish policy and procedures for the conduct of authorized CI activities by NCIS CI personnel per reference (d) and this instruction.

3 Jan 17

n. Per paragraph 5 of this instruction, ensure NCIS CI elements and activities are coordinated, synchronized, and de-conflicted with USN and USMC CI elements.

o. In coordination with DNI and DIRINT, ensure CI activities are integrated into all operations, programs, systems, exercises, plans, doctrines, strategies, policies, and architectures of the DON and its components.

p. Develop and implement CI awareness briefings, threat mitigation activities and reporting procedures, per references (b), (g), (m), and (t), such that all CI incidents, including questionable intelligence activities, within the DON are reported to the UNSECNAV and USD(I) per references (e) and (i).

q. Assign a senior CI-trained Special Agent to the DON Secretariat, CNO and CMC Staff; and to the staff of each component command, fleet, and Marine Expeditionary Force as appropriate.

r. Ensure USN and USMC component commanders are properly supported and apprised of NCIS CI activities through the cognizant CI staff officer or CI/Human Intelligence officer. Provide USN and USMC component commanders any CI reports or CI/Counter Terrorism information that could impact USN and/or USMC forces.

s. Ensure DON interoperability of intelligence, CI, and law enforcement related databases, systems, and capabilities to the maximum extent possible.

t. Identify to the UNSECNAV, GC, DUSN (P), DNI, and DIRINT those DON forces, operations, programs, facilities, equipment, and networks requiring additional or tailored CI support.

u. Per references (u) and (v), manage the DON Technical Surveillance Countermeasure Program.

v. Per reference (s), manage the DON CI polygraph and credibility assessment service programs.

3 Jan 17

w. In consultation with the UNSECNAV, GC, and DUSN(P), establish procedures for coordination of CI collection activities within the DON and the employment of the Multiple Threat Alert Center for CI collection management, analysis, and production support to the DON and its components.

x. Provide CI support to USN, USMC, Combatant Commands, and other DoD Components as directed by SECNAV or UNSECNAV.

y. Represent DON CI interest in national forums and pertinent CI and law enforcement groups after consultation with UNSECNAV, GC, and DUSN (P).

z. Provide CI support to cyber operations, including but not limited to, digital forensics and cyber vulnerability assessments per reference (t).

aa. Ensure no CI activities be delayed if they involve fleeting opportunities, perishable information, or risk of loss of life. In those cases, NCIS CI elements will coordinate with the respective USN or USMC component CI personnel at the earliest opportunity, but in no case shall that time limit exceed eight days.

ab. Unless prohibited by other authority, inform UNSECNAV, GC, and DUSN (P) of all significant CI issues affecting the DON in a timely manner. In those instances involving USN or USMC personnel, also inform the DNI or DIRINT as appropriate and per references (f), (g), and (w).

ac. Integrate CI capabilities, information, and support into NCIS plans, operations, and activities.

ad. Provide for the conduct of CI activities responsive to NCIS requirements.

ae. Implement the policies and procedures contained in this instruction.

af. Ensure the UNSECNAV, GC, DUSN (P), NAVINSGEN, IGMC, and members of the SRB are kept fully and currently

3 Jan 17

informed of significant and/or sensitive DON intelligence and CI activities, questionable CI activities, and intelligence-related activities using any DON non-intelligence component assets, including personnel and equipment per reference (x). Such notification shall occur in writing within 48 hours of any activity.

ag. Ensure all subordinate intelligence and CI components, activities, units, and elements in NCIS comply with the requirements of this instruction and references.

5. The DNI shall:

a. Serve as the principal advisor to the CNO for CI and Intelligence matters.

b. Ensure CI requirements are identified, documented, and reported to the UNSECNAV, GC, DUSN (P), and DIRNCIS on an annual basis and as required.

c. Exercise authority, direction, and control over USN CI personnel and activities, unless such personnel are assigned to NCIS.

d. Direct the conduct of CI activities in support of USN requirements.

e. Ensure CI requirements beyond USN capacity or authority are identified and presented to the UNSECNAV, GC, DUSN (P), NCIS, and DIRINT for coordination and support.

f. Identify to the UNSECNAV, GC, DUSN (P), and DIRNCIS those USN forces, operations, programs, facilities, equipment, and networks requiring additional or tailored CI support.

g. Serve as the resource sponsor for USN and NCIS CI activities and provide quarterly accounting and execution reports to the UNSECNAV, GC, and DUSN (P).

h. Organize, train, and equip USN CI personnel.

3 Jan 17

- i. Per references (f), (g), (l), (r), and (s), maintain a database of all issued CI credentials for USN personnel, and provide a record of credentials to the DIRNCIS.
- j. Establish policy and procedures for the conduct of authorized CI activities by USN CI personnel per references (a) through (ag), and this instruction.
- k. Per paragraph 5 of this instruction, ensure USN CI elements and activities are coordinated, synchronized, and de-conflicted with NCIS CI and USMC elements.
- l. Ensure CI activities are integrated into all operations, programs, systems, exercises, plans, doctrine, strategies, policies, and architectures of the USN and its components assigned to the GCCs.
- m. Develop and implement CI awareness briefings, threat mitigation activities, and reporting procedures for the USN, per references (b), (g), (m), and (t), such that all CI incidents within the USN are reported to DIRNCIS per references (e) and (i).
- n. Represent USN CI interest (less Law Enforcement) in national forums and pertinent IC groups.
- o. Provide CI support to cyber operations, including but not limited to, digital forensics and cyber vulnerability assessments per reference (t) and this instruction.
- p. Ensure no CI activities be delayed if they involve fleeting opportunities, perishable information, or risk of loss of life. In those cases, ensure USN CI elements coordinate with the NCIS CI element at the earliest opportunity, but in no case shall that time limit exceed eight calendar days.
- q. Inform the UNSECNAV, GC, DUSN (P), and DIRNCIS of all significant CI issues affecting the USN in a timely manner per references (f), (g), and (w).

3 Jan 17

r. Integrate CI capabilities, information, and support into USN plans, operations, and activities.

s. Provide for the conduct of CI activities responsive to USN requirements.

t. Implement the policies and procedures contained in this instruction.

u. Ensure the UNSECNAV, GC, DUSN (P), NAVINSGEN, IGMC, and members of the SRB, are kept fully and currently informed of significant and/or sensitive DON intelligence and CI activities, questionable CI activities, and intelligence-related activities using any DON non-intelligence component assets, including personnel and equipment per reference (x). Such notification shall occur in writing within 48 hours of any activity.

v. Ensure all subordinate intelligence and CI components, activities, units, and elements in the USN comply with the requirements of this instruction and references.

6. The DIRINT, Headquarters Marine Corps shall:

a. Serve as the principal advisor to the CMC for CI and intelligence matters.

b. Ensure USMC CI requirements are identified, documented, and reported to the UNSECNAV, GC, DUSN (P), and DIRNCIS on an annual basis or as required.

c. Exercise authority, direction, and control over USMC CI personnel and activities, unless such personnel are assigned to NCIS.

d. Direct the conduct of CI activities in support of USMC requirements.

e. Ensure CI requirements beyond USMC capacity or authority are identified and presented to the UNSECNAV, GC, DUSN (P), DIRNCIS, and DNI for coordination and support.

3 Jan 17

f. Identify to the UNSECNAV, GC, DUSN (P), and DIRNCIS those USMC forces, operations, programs, facilities, equipment, and networks requiring additional or tailored CI support.

g. Serve as the resource sponsor for all USMC CI activities and provide quarterly accounting and execution reports to the UNSECNAV, GC, and DUSN (P).

h. Organize, train, and equip USMC CI personnel.

i. Per references (f), (g), (l), (r), and (s), maintain a database of all issued CI credentials for USMC personnel, and provide a record of credentials to the DIRNCIS.

j. Establish policy and procedures for the conduct of authorized CI activities by USMC CI personnel per references (a) through (ag), and this instruction.

k. Per paragraph 5 of this instruction, ensure USMC CI elements and activities are coordinated, synchronized, and de-conflicted with USN and NCIS CI elements.

l. Ensure CI activities are integrated and coordinated into all operations, programs, systems, exercises, plans, doctrine, strategies, policies, and architectures of the USMC and its components.

m. Develop and implement CI awareness briefings, threat mitigation activities, and reporting procedures for the USMC, per references (b), (g), (m), and (t) such that all CI incidents within the USMC are reported to DIRNCIS per references (e) and (i).

n. Represent USMC CI and related interest (less Law Enforcement) in national forums and pertinent IC groups.

o. Provide CI support to cyber operations, including but not limited to, digital forensics and cyber vulnerability assessments per reference (t) and this instruction.

3 Jan 17

p. Ensure no CI activities be delayed if they involve fleeting opportunities, perishable information, or risk of loss of life. In those cases, ensure USMC CI elements coordinate with the NCIS CI element at the earliest opportunity, but in no case shall that time limit exceed eight calendar days.

q. Inform the UNSECNAV, GC, DUSN (P), and DIRNCIS of all significant CI issues affecting the USMC in a timely manner and per references (f), (g), and (w).

r. Integrate CI capabilities, information, and support into USMC plans, operations, and activities.

s. Provide for the conduct of CI activities responsive to USMC requirements.

t. Implement the policies and procedures contained in this instruction.

u. Ensure the UNSECNAV, GC, DUSN (P), NAVINSGEN, IGMC, and members of the SRB, are kept fully and currently informed of significant and/or sensitive DON intelligence and CI activities, questionable CI activities, and intelligence-related activities using any DON non-intelligence component assets, including personnel and equipment per reference (x). Such notification shall occur in writing within 48 hours of any activity.

v. Ensure all subordinate intelligence and CI components, activities, units, and elements in the USMC comply with the requirements of this instruction and references.