



# Department of Defense INSTRUCTION

NUMBER O-3115.07

September 15, 2008

*Incorporating Change 1, November 19, 2010*

USD(I)

SUBJECT: Signals Intelligence (SIGINT)

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. Reissues DoD Directive (DoDD) S-3115.7 (Reference (a)) as a DoD Instruction (DoDI) in accordance with the guidance in DoDI 5025.01 (Reference (b)) and the authorities in DoDD 5143.01 (Reference (c)), DoDD 5100.20 (Reference (d)), DoDD 5240.1 (Reference (e)), and DoD Regulation 5240.1-R (Reference (f)).

b. Updates SIGINT policy, definitions, and responsibilities within the Department of Defense.

c. Shall conform to and be consistent with the law and Presidential guidance concerning the authorities and responsibilities of the Director of National Intelligence (DNI) in accordance with the National Security Act of 1947 as amended (Reference (g)), Executive Order 12333 (Reference (h)), and Intelligence Community Directive 300 (Reference (i)).

2. APPLICABILITY. This Instruction applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint 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 within the Department of Defense (hereafter referred to collectively as the "DoD Components").

b. Pursuant to the Foreign Intelligence Surveillance Act (Reference (j)) and National Security Council Intelligence Directive No. 6 (Reference (k)), the United States Coast Guard (USCG) and other non-DoD entities that are conducting SIGINT under Secretary of Defense authority.

~~FOR OFFICIAL USE ONLY~~

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. SIGINT operations and activities shall be treated as high priority efforts and receive full and pro-active support in all resourcing and programmatic actions.

b. Pursuant to Reference (h), the Director, National Security Agency, (DIRNSA) is designated the Functional Manager for SIGINT.

c. No other department or agency may engage in SIGINT activities except pursuant to a delegation by the Secretary of Defense, after coordination with the DNI (Reference (h)).

d. Pursuant to Reference (i), SIGINT instructions on collection, processing, analysis, production, and dissemination activities issued by the DIRNSA/Chief, Central Security Service (CSS) (CHCSS), shall be mandatory for all DoD Components and other non-DoD entities that are conducting SIGINT under Secretary of Defense authority, subject to an appeal to the Secretary of Defense. This appeal adjudication is hereby delegated to the Under Secretary of Defense for Intelligence (USD(I)).

e. Electronic surveillance as defined in Reference (j) shall be conducted in accordance with References (f) and (j).

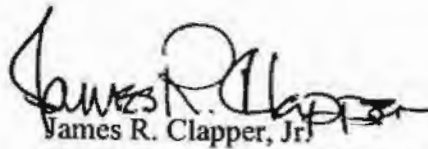
5. RESPONSIBILITIES. See Enclosure 2.

6. INFORMATION REQUIREMENTS. Intelligence continuity plans, including all response mechanisms and reporting requirements referred to in this Instruction, are exempt from licensing in accordance with paragraphs C4.4.2. through C4.4.4. of DoD 8910.1-M (Reference (I)).

7. RELEASABILITY. RESTRICTED. This Instruction is approved for restricted release. ~~The DoD Components (to include the Combatant Commands) and other Federal agencies may obtain copies of this Instruction through controlled Internet access from the DoD Directives Program Web Site on the SECRET Internet Protocol Network at <http://www.dtic.smil.mil/whs/directives>. It is available to users with Common Access Card authorization on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.~~

*Change 1, 11/19/2010*

8. EFFECTIVE DATE. This Instruction is effective immediately.



James R. Clapper, Jr.  
Under Secretary of Defense for Intelligence

Enclosures

1. References
  2. Responsibilities
- Glossary

*Change 1, 11/19/2010*



TABLE OF CONTENTS

REFERENCES .....5

RESPONSIBILITIES .....6

    USD(I).....6

    DIRNSA/CHCSS .....7

    DIRECTOR, NATIONAL RECONNAISSANCE OFFICE (NRO) .....10

    DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA).....11

    UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY,  
    AND LOGISTICS (USD(AT&L)) .....12

    ASSISTANT SECRETARY OF DEFENSE FOR SPECIAL OPERATIONS/  
    LOW INTENSITY CONFLICT AND INTERDEPENDENT CAPABILITIES  
    (ASD(SOLIC&IC)).....12

    GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE.....12

    HEADS OF THE DOD COMPONENTS.....12

    SECRETARIES OF THE MILITARY DEPARTMENTS AND  
    COMMANDANT, USCG .....13

    COMMANDANT, USCG .....14

    CHAIRMAN OF THE JOINT CHIEFS OF STAFF.....15

    COMMANDERS OF THE COMBATANT COMMANDS AND  
    COMMANDANT, USCG .....15

    COMMANDER, USSTRATCOM .....16

    COMMANDER, USSOCOM.....16

GLOSSARY .....17

    ABBREVIATIONS AND ACRONYMS .....17

    DEFINITIONS.....18

ENCLOSURE 1

REFERENCES

- (a) DoD Directive S-3115.7, "Signals Intelligence (SIGINT) (U)," January 25, 1973 (hereby canceled)
- (b) DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007
- (c) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),  
November 23, 2005
- (d) DoD Directive 5100.20, "The National Security Agency and the Central Security Service,"  
December 23, 1971
- (e) DoD Directive 5240.01, "DoD Intelligence Activities," August 27, 2007
- (f) DoD Regulation 5240.1-R, "Procedures Governing the Activities of DoD Intelligence  
Components that Affect United States Persons," December 1, 1982
- (g) National Security Act of 1947, as amended
- (h) Executive Order 12333, "United States Intelligence Activities," as amended
- (i) Intelligence Community Directive 300, "Management, Integration, and Oversight of  
Intelligence Collection, and Covert Actions," October 3, 2006<sup>1</sup>
- (j) "Foreign Intelligence Surveillance Act," as amended
- (k) National Security Council Intelligence Directive No. 6, "Signals Intelligence,"  
February 17, 1972
- (l) DoD 8910.1-M, "Department of Defense Procedures for Management of Information  
Requirements," June 30, 1998
- (m) Deputy Secretary of Defense Memorandum, "Authorities for the Military Intelligence  
Program," December 20, 2005<sup>2</sup>
- (n) DoD Instruction 3305.09, "DoD Cryptologic Training," December 22, 2006
- (o) DoD Directive 5105.23, "National Reconnaissance Office," March 27, 1964
- (p) Memorandum of Agreement between the Director of National Intelligence and the  
Secretary of Defense, "Management of Acquisition Programs Executed at the Department  
of Defense Community Elements," March 25, 2008<sup>2</sup>

<sup>1</sup> Copies of this document are available via the Defense ~~SECRET~~ Internet Protocol Router Network through  
USDI.Pubs@osd.smil.mil

<sup>2</sup> Available from [https://usdi.dtic.mil/usdi\\_docs/keyref/usdi\\_keyref.cfm](https://usdi.dtic.mil/usdi_docs/keyref/usdi_keyref.cfm)



ENCLOSURE 2

RESPONSIBILITIES

1. USD(I). In accordance with References (c) and (h), the Secretary of Defense, as the executive agent for SIGINT and the senior DoD official who coordinates SIGINT responsibilities with the DNI, has delegated responsibility for exercising authority, direction, and control over the DIRNSA/CHCSS to the USD(I). The USD(I), who also serves as the program executive for the approval of Military Intelligence Program (MIP) related actions pursuant to Deputy Secretary of Defense Memorandum (Reference (m)), shall:

a. Serve as the principal staff assistant to the Secretary of Defense pursuant to Reference (c) and as the primary DoD representative to the Office of the Director of National Intelligence (ODNI) for defense intelligence issues.

b. Exercise authority, direction, control, and fiscal management over the National Security Agency/Central Security Service (NSA/CSS) and exercise policy and strategic oversight over SIGINT policy, plans, and programs, to include the directives and policies of NSA/CSS and other DoD Components involved in SIGINT activities.

c. Coordinate the development of a SIGINT Roadmap for the future with NSA/CSS and other DoD Components engaged in SIGINT activities.

d. Coordinate, assess, and deconflict SIGINT-related MIP requirements in association with National Intelligence Program (NIP) requirements.

e. Exercise planning and policy oversight of human capital so that SIGINT activities are manned, trained, equipped, and structured by the Military Departments to support national requirements and DoD missions and fully satisfy the needs of the President, the National Security Council, the Intelligence Community (IC), and the Combatant Commands.

(1) Develop policy and procedures on matters pertaining to the establishment, management, and training of a SIGINT career force in coordination with other DoD Components, as appropriate, and in accordance with DoDI 3305.09 (Reference (n)).

(2) Provide training policy and oversight as it pertains to United States Joint Forces Command integration of SIGINT capabilities into joint exercises and joint training in coordination with the DoD Components.

f. In coordination with the Chairman of the Joint Chiefs of Staff and the Director, Defense Intelligence Operations Coordination Center (DIOCC), evaluate DIRNSA/CHCSS SIGINT plans and programs for adequacy and responsiveness in support of intelligence planning and provide direction and guidance to the DIRNSA/CHCSS.

2. DIRNSA/CHCSS. The DIRNSA/CHCSS, under the authority, direction, and control of the USD(I), shall:

a. Serve as the principal SIGINT advisor to the Secretary of Defense, the USD(I), the Chairman of the Joint Chiefs of Staff, the Combatant Commanders, and the DNI, reporting to the Secretary of Defense through the USD(I), and keeping them fully informed of SIGINT matters.

b. When acting as the SIGINT Functional Manager in accordance with Reference (h), the DIRNSA shall report to the DNI concerning the execution of his or her duties as the SIGINT Functional Manager. In such instances, the DIRNSA should inform the USD(I) of these discussions.

c. Supervise, fund, maintain, and operate NSA/CSS and the United States SIGINT System (USSS) as a jointly-staffed, unified SIGINT organization; exercise control of all SIGINT collection, processing, analysis, production, and dissemination activities of the United States in accordance with References (d), (h), and (k).

d. Provide SIGINT collection, processing, analysis, production, and dissemination activities to support the conduct of military operations in accordance with tasking priorities and standards of timeliness assigned by the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Combatant Commanders. If the provision of such support requires use of national collection systems, these systems shall be tasked consistent with the provisions of Reference (h).

e. Respond to SIGINT-related requirements (e.g., SIGINT collection, processing, analysis, production, dissemination, and other SIGINT issues) in support of the DoD Components, to include planning, operations, assessments, requests for technical information, and other support as required.

f. Collect, process, analyze, produce, and disseminate SIGINT for foreign intelligence in accordance with the objectives, requirements, and priorities established by the DNI, in accordance with Reference (h).

g. Collect, process, analyze, produce, and disseminate SIGINT for counterintelligence purposes, in accordance with Reference (h).

h. ~~(FOUO)~~ Ensure that the capabilities resident in SIGINT activities designated for wartime or contingency deployment are productively used during peacetime in support of appropriate SIGINT and readiness requirements.

i. Provide appropriate SIGINT support to National Intelligence Support Plans.

j. Exercise SIGINT operational control over SIGINT activities of the USSS in accordance with Reference (d) to respond most effectively to military and other SIGINT requirements by:



(1) Delegating standing SIGINT operational tasking authority (SOTA) to the Military Departments, the Commandant of the Marine Corps, and the Commandant of the USCG with organic SIGINT units permanently assigned under their command.

(2) Delegating temporary SOTA through the Chairman of the Joint Chiefs of Staff to the Combatant Commanders, subordinate component commanders, joint task forces, and directly to the Service cryptologic components (SCC) on a case-by-case, mission-specific basis to permit those commanders (or delegated representatives) to directly task designated SIGINT units, platforms, and assets assigned to their command to achieve their mission objectives in a timely and efficient manner, and coordinating these actions with the SCCs so as not to impinge upon the capabilities of organic tactical SIGINT units to provide required support to their parent Service.

(3) Approving SIGINT missions for military SIGINT units, platforms, or other assets assigned to and under the operational control of a military commander.

(4) Levying SIGINT advisory tasking against military units, platforms, or other assets that have SIGINT capabilities but whose primary purpose is not SIGINT collection, processing, or other SIGINT-related activities. This tasking must:

(a) Have the concurrence of the affected commander;

(b) Not interfere with the primary purpose of the resource or the mission of the command to which it is assigned; and

(c) Provide guidance to ensure the resulting SIGINT product is provided to the designated NSA/CSS office or activity as soon as possible.

(5) Levying SIGINT supplemental tasking against military SIGINT units, platforms, or other assets for which SOTA has been delegated to a military commander with the concurrence of the affected commander.

(6) Retaining SIGINT operational control of all SIGINT resources fulfilling national SIGINT requirements.

(7) Apprising the Combatant Command Joint Intelligence Operations Centers (JIOCs) and DIOCC of all SIGINT-related activities relevant to their respective responsibilities.

k. Upon approval by the USD(I), develop and implement SIGINT programs, plans, policies, procedures, principles, and guidance for DoD elements engaged in SIGINT activities in accordance with DoD policies and guidance to:

(1) Provide technical guidance for the collection, processing, analysis, production, and dissemination of SIGINT.

(2) Issue SIGINT operational and technical policy to carry out DIRNSA/CHCSS responsibilities and functions to units involved in SIGINT operations, keeping the USD(I) and

*Change 1, 11/19/2010*



the DNI informed. This includes issuing instructions and policy related to the collection, processing, analysis, production, retention, dissemination, and assessment of SIGINT information.

(3) Exercise the necessary monitoring and supervisory control to ensure compliance with DoD and DNI issuances prescribing security regulations and with directives covering SIGINT operating practices including the transmission, handling, and distribution of SIGINT material.

1. Standardize SIGINT equipment, processes, and facilities; eliminate unwarranted duplication of SIGINT efforts, where practical, in coordination with the Military Departments.

m. Manage assigned DoD and national SIGINT resources, personnel, and programs to assure consistency and interoperability with the NIP, as appropriate; maintain consistency with architectures and standards; and conduct assessments to ensure mission accomplishment. In this capacity, the DIRNSA/CHCSS shall:

(1) Act as the Program Manager of the NSA MIP as directed in MIP implementation guidance.

(2) Manage the development of all Service, United States Strategic Command (USSTRATCOM), and United States Special Operations Command (USSOCOM) SIGINT investment programs, excluding budgetary approval. In the event of an issue or disagreement, the concerned party may submit an appeal to the USD(I) for resolution.

(3) Provide architectural standards, compliance, and interoperability assessments to assist milestone decision authorities in production decisions.

(4) Recommend adjustments to SCC personnel resources under DIRNSA/CHCSS SIGINT operational control and convey these adjustments to the SCC commanders, as required. Pursuant to Reference (c), the USD(I) shall adjudicate any disagreements between the SCC commanders and the DIRNSA/CHCSS regarding personnel resources.

(5) Prepare and submit to the DNI, after coordination with the USD(I), the NSA/CSS NIP Consolidated Cryptologic Program budget and list of requirements for military and civilian manpower; logistics; communications support; and research, development, testing, and evaluation (RDT&E), together with pertinent recommendations.

(6) Provide the DNI, in coordination with the USD(I), past, current, and proposed plans, programs, and costs of the SIGINT activities under DIRNSA/CHCSS control.

(7) Provide personnel, to include senior representatives, and resources in direct support to the Combatant Command JIOCs and DIOCC for direct support of their missions.

(8) Provide personnel and resources for SIGINT indications and warning of potential foreign threats to DoD telecommunications and information systems.

n. Conduct RDT&E to meet the needs of the USSS by:

(1) Managing DoD SIGINT RDT&E investments for technologies, programs, and product support consistent with Reference (h) as part of the requirements, planning, programming, budgeting, and acquisition processes. These efforts shall be in coordination with the Military Departments while recognizing the authority of USSOCOM to input their respective requirements into the development process. In the event of a disagreement, the concerned party may submit an appeal to the USD(I) for resolution.

(2) Providing technical advice, assistance, and guidance, consistent with enterprise architecture and interoperability standards established by the IC Chief Information Officer in accordance with Reference (h), to the Military Departments, USSTRATCOM, and USSOCOM for SIGINT RDT&E investment programs to ensure architecture, standards, and interoperability between existing and future Military Department and USSOCOM SIGINT systems; connectivity between national and tactical systems; and modernization of systems.

(3) Coordinate with other DoD, USCG and, as appropriate, IC components concerning SIGINT RDT&E investment techniques, procedures, and equipment resulting from SIGINT and non-SIGINT RDT&E programs.

o. Provide guidance to the Military Departments and the USCG for military and civilian SIGINT career development and training programs and conduct, or otherwise provide for, necessary specialized and advanced SIGINT training. This should include established policies, standards, and procedures to ensure the technical adequacy of SIGINT training within the Department of Defense in accordance with References (d) and (n).

p. Arrange, as necessary, the conduct and support of SIGINT activities outside the Department of Defense in accordance with References (h) and (k).

q. In accordance with Reference (h), conduct foreign cryptologic liaison relationships.

3. DIRECTOR, NATIONAL RECONNAISSANCE OFFICE (NRO). The Director, NRO, under the authority, direction, and control of the USD(I), shall:

a. In partnership with the DIRNSA, as appropriate, perform the NRO statutory duty in accordance with DoDD 5105.23 (Reference (o)) of researching, developing, acquiring, launching, and maintaining the operational capability of national space-based SIGINT collection systems to meet DoD and IC requirements.

b. In coordination with the DIRNSA/CHCSS and the Commander, USSTRATCOM, as appropriate, provide fact-based, architectural-related recommendations to the DNI and the USD(I) for sound business and mission decisions in relation to current and future SIGINT processing systems architecture.



4. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). The Director, DIA, under the authority, direction, and control of the USD(I), shall:

a. Manage DoD SIGINT-related intelligence requirements to support DoD all-source intelligence and counterintelligence collection, production, analysis, and dissemination.

b. Collaborate with the Chairman of the Joint Chiefs of Staff, the Military Departments, and the Combatant Commands to develop mechanisms to evaluate the contribution of SIGINT in relation to commander priority information requirements during the production of finished intelligence; provide recommendations to the DIRNSA.

c. Perform analyses of foreign counter-SIGINT threats in coordination with NSA/CSS and other DoD and Government agencies as appropriate.

d. In his or her role as the Director, DIOCC:

(1) Maintain awareness of SIGINT requirements and ongoing operations for which the DIRNSA/CHCSS has delegated SOTA to the Military Departments, the Commandant of the Marine Corps, the Combatant Commands, and the USCG.

(2) In conjunction with the USSTRATCOM Joint Functional Component Command – Intelligence, Surveillance, and Reconnaissance (JFCC-ISR), coordinate intelligence requirements, including SIGINT, for the Combatant Commands and the Military Services. Formulate recommended solutions to deconflict and satisfy requirements for national intelligence; coordinate all SIGINT solutions with the DIRNSA and the National Intelligence Coordination Center (NICC).

(3) In conjunction with JFCC-ISR, coordinate with the Combatant Commands to synchronize DoD intelligence, surveillance, and reconnaissance resources with other collection activities, including SIGINT.

(4) Identify and evaluate competing SIGINT requirements across the Combatant Commands. Communicate with NSA, the Combatant Commands, Military Services, DIA, NRO, and NICC to coordinate SIGINT collection and resolve competition for resources.

(5) Monitor planning and execution of SIGINT support to National Intelligence Support Plans.

(6) Accept and integrate NSA/CSS representation into DIOCC to facilitate SIGINT tasking, coordination, and requirements resolution.

(7) Provide to NSA/CSS validated defense intelligence requirements and recommend prioritization.

5. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS (USD(AT&L)). The USD(AT&L) shall:

a. Establish policies for the acquisition of SIGINT systems in coordination with the DNI, the USD(I), the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the DIRNSA/CHCSS, and others, as appropriate. Major system acquisitions that are majority-funded by the NIP shall be executed in accordance with the Memorandum of Agreement between the DNI and the Secretary of Defense, "Management of Acquisition Programs Executed at the Department of Defense Community Elements" (Reference (p)).

b. Develop and maintain a DoD science and technology investment strategy to support the development, acquisition, and integration of technological advances in tactical SIGINT systems and platforms managed by the Military Departments.

c. Incorporate countermeasures to technical surveillance and exploitation in SIGINT acquisition programs.

6. ASSISTANT SECRETARY OF DEFENSE FOR SPECIAL OPERATIONS/LOW INTENSITY CONFLICT AND INTERDEPENDENT CAPABILITIES (ASD(SOLIC&IC)).

The ASD(SOLIC&IC), under the authority, direction, and control of the Under Secretary of Defense for Policy, shall review all USSOCOM investment program requests and provide recommendations to the DIRNSA/CHCSS.

7. GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE. The General Counsel of the Department of Defense shall:

a. Provide legal advice and assistance to the Secretary of Defense, the USD(I), the NSA General Counsel, the ODNI General Counsel, and other OSD organizations.

b. Oversee, as appropriate, the legal services performed within the Department of Defense, including those provided by the general counsels and legal advisers within the Defense Intelligence Components.

c. Provide for the coordination of legal issues, as appropriate, with the NSA General Counsel, the Department of Justice, the ODNI General Counsel, and other departments and agencies.

8. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall assign responsibilities and establish procedures, as appropriate, within their organizations to implement this Instruction.



9. SECRETARIES OF THE MILITARY DEPARTMENTS AND COMMANDANT, USCG.

The Secretaries of the Military Departments and the Commandant, USCG, shall:

- a. Plan and program for defense SIGINT capabilities under the guidance of the USD(I) and in coordination with the DIRNSA/CHCSS.
- b. Designate an SCC commander for each Military Service and provide military personnel to NSA/CSS to perform NSA/CSS-assigned SIGINT missions in accordance with approved requirements and procedures.
- c. Operate and maintain SIGINT facilities and resources, in coordination with NSA/CSS, for the conduct and support of SIGINT operations as authorized and directed by the Secretary of Defense or the USD(I), including military Reserve programs to meet emergency or wartime requirements for SIGINT resources.
- d. Coordinate SIGINT investment programs with the DIRNSA/CHCSS. In the event of an issue or disagreement with the DIRNSA/CHCSS, submit an appeal to the USD(I) for resolution.
- e. Develop network-enabled SIGINT equipment that meets architecture standards and is interoperable with national SIGINT systems, other Military Department tactical SIGINT systems, and JIOC operating systems, as necessary.
- f. As appropriate and in accordance with guidance from the DIRNSA/CHCSS, through the respective Military Department SIGINT and training organizations, conduct SIGINT activities, training, and operations in support of military commanders and the DIRNSA/CHCSS.
- g. Assist NSA/CSS in conducting SIGINT-related research and development to meet the needs of the United States for SIGINT by:
  - (1) Coordinating RDT&E requirements with the DIRNSA/CHCSS.
  - (2) Accomplishing specified RDT&E tasks within approved programs as requested by the DIRNSA/CHCSS and in accordance with DoD guidance and direction.
  - (3) Maintaining a system in coordination with the DIRNSA/CHCSS to support SIGINT management by reporting program execution data to NSA/CSS.
  - (4) Performing threat analysis and coordinating with other DoD Components, as necessary, to incorporate SIGINT threat countermeasures in acquisition and RDT&E programs.
- h. Coordinate, plan, program, budget, maintain, and conduct SIGINT training in accordance with Reference (n) and USD(I) policy and guidance.
- i. Submit SIGINT information requirements to DIA, simultaneously providing information copies to NSA/CSS. In addition, submit time-sensitive or otherwise urgent SIGINT information needs directly to NSA/CSS, simultaneously informing DIOCC.

*Change 1, 11/19/2010*

13

ENCLOSURE 2

~~FOR OFFICIAL USE ONLY~~

10. COMMANDANT, USCG. In addition to the responsibilities in sections 9 and 12, the Commandant, USCG, shall:

a. Plan and program for SIGINT resources in consonance with fiscal policy and guidance established by the Secretary of Homeland Security and program guidance received from the DNI, the USD(I), and the DIRNSA/CHCSS.

b. Provide military personnel to NSA/CSS to perform NSA/CSS-assigned SIGINT missions in accordance with approved requirements and procedures.

c. Operate and maintain SIGINT facilities and resources, in coordination with NSA/CSS, for the conduct and support of SIGINT operations as authorized and directed by the Secretary of Defense or the USD(I).

d. Submit tactical SIGINT investment programs for DIRNSA concurrence.

e. Develop network-enabled SIGINT equipment that meets architecture standards and is fully interoperable with national SIGINT systems, other Military Department tactical SIGINT systems, and JIOC operating systems.

f. As appropriate, and in accordance with guidance from the DIRNSA/CHCSS and through the respective Military Department SIGINT and training organizations, conduct SIGINT activities, training, and operations in support of military commanders and the DIRNSA/CHCSS.

g. Assist NSA/CSS in conducting SIGINT-related research and development to meet the needs of the United States for SIGINT by:

(1) Coordinating RDT&E requirements with the DIRNSA/CHCSS.

(2) Accomplishing specified RDT&E tasks within approved programs as requested by the DIRNSA/CHCSS and in accordance with DoD guidance and direction.

(3) Maintaining a system in coordination with the DIRNSA/CHCSS to support SIGINT management by reporting program execution data to NSA/CSS.

(4) Performing threat analysis and coordinating with the DoD Components, as necessary, to incorporate SIGINT threat countermeasures in acquisition and RDT&E programs.

h. Coordinate, plan, program, budget, maintain, and conduct SIGINT training in accordance with Reference (i) and USD(I) policy and guidance.

i. Submit SIGINT information requirements to NSA/CSS, simultaneously providing information copies to the Director, JIOC.



11. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. The Chairman of the Joint Chiefs of Staff shall:

- a. Monitor USSS responsiveness to military requirements and make recommendations to the Secretary of Defense.
- b. Respond to, coordinate, and allocate resources to fulfill Combatant Commander requests for military SIGINT platforms, units, or other assets, to include delegation of SOTA by the DIRNSA/CHCSS, if required, for allocated SIGINT resources.
- c. Validate joint and Military Department SIGINT system and platform requirements through appropriate DoD and Joint Staff processes.
- d. Develop and maintain joint doctrine for core, supporting, and related SIGINT capabilities in joint operations.
- e. Submit SIGINT information requirements to DIA, simultaneously providing information copies to NSA/CSS. In addition, submit time-sensitive or otherwise urgent SIGINT information needs directly to NSA/CSS, simultaneously informing DIOCC.

12. COMMANDERS OF THE COMBATANT COMMANDS AND COMMANDANT, USCG. The Commanders of the Combatant Commands and the Commandant, USCG, shall:

- a. Integrate, plan, and execute SIGINT operations in support of intelligence planning, approved military plans, and other operations in conjunction with NSA/CSS.
- b. Submit SIGINT information requirements to DIA, simultaneously providing an information copy to NSA/CSS. In addition, submit time-sensitive or otherwise urgent SIGINT information requirements directly to NSA/CSS, simultaneously informing DIOCC.
- c. Submit to the Chairman of the Joint Chiefs of Staff requests for military SIGINT platforms, units, or other assets, simultaneously informing DIOCC. As feasible, the Commanders of the Combatant Commands should request SOTA as part of these submissions.
- d. Exercise operational control of military platforms, units, or other assets that have a SIGINT capability in accordance with established procedures or supplemental instructions issued by the Joint Chiefs of Staff, taking into consideration the SIGINT advisory and supplemental tasking of the DIRNSA/CHCSS, if appropriate.
- e. ~~FOUO~~ Ensure compartmented SIGINT operations are provided adequate protection from disclosure; exercise SIGINT units in direct support of compartmented operations as directed by the Secretary of Defense.
- f. Where not otherwise delegated, submit requests for SOTA delegations of SIGINT resources to the DIRNSA/CHCSS subject to an appeal to the USD(I).

*Change 1, 11/19/2010*

15

ENCLOSURE 2

~~FOR OFFICIAL USE ONLY~~

g. Assume SOTA of SIGINT resources when delegated by the DIRNSA/CHCSS.

h. Forward to the DIRNSA/CHCSS all SIGINT products and SIGINT technical data resulting from the tasking of SIGINT resources under Combatant Commander and USCG operational control and for which the DIRNSA/CHCSS has delegated SOTA to the Combatant Commander.

i. Apprise the Secretary of Defense, the USD(I), the Chairman of the Joint Chiefs of Staff, the DIRNSA/CHCSS, and the Director, DIOCC, of the operational status of all allocated SIGINT resources.

j. Monitor USSS responsiveness to military requirements and make recommendations to the Chairman of the Joint Chiefs of Staff.

k. Accept and integrate NSA/CSS representation into the respective JIOCs or their equivalent to facilitate SIGINT tasking, coordination, and requirements resolution.

13. COMMANDER, USSTRATCOM. In addition to the responsibilities in section 12, the Commander, USSTRATCOM, shall:

a. Apprise the Secretary of Defense, the USD(I), the Chairman of the Joint Chiefs of Staff, and the DIRNSA/CHCSS of the status of the allocated SIGINT resources of the Combatant Commands, simultaneously informing DIA.

b. Coordinate SIGINT investment programs with the DIRNSA. In the event of an issue or disagreement with the DIRNSA/CHCSS, submit an appeal to the USD(I) for resolution.

c. As military lead for the Battlespace Awareness Capability Portfolio Manager and in coordination with the Joint Staff Director of Intelligence/J2, recommend and advocate Combatant Command SIGINT needs.

14. COMMANDER, USSOCOM. In addition to the responsibilities in section 12, the Commander, USSOCOM, in coordination with the DIRNSA/CHCSS, shall, within directed responsibilities, develop special operations forces-unique SIGINT equipment that is network-enabled, fits architecture, meets standards, and is interoperable with national SIGINT systems and other Military Department tactical SIGINT systems in accordance with appropriate DoD and Joint Staff processes.



GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(SOLIC&IC)	Assistant Secretary of Defense for Special Operations/Low Intensity Conflict and Interdependent Capabilities
CHCSS	Chief, Central Security Service
CSS	Central Security Service
DIA	Defense Intelligence Agency
DIOCC	Defense Intelligence Operations Coordination Center
DIRNSA	Director, National Security Agency
DNI	Director of National Intelligence
DoDD	DoD Directive
DoDI	DoD Instruction
IC	Intelligence Community
JFCC-ISR	Joint Functional Component Command – Intelligence, Surveillance, and Reconnaissance
JIOC	Joint Intelligence Operations Center
MIP	Military Intelligence Program
NICC	National Intelligence Coordination Center
NIP	National Intelligence Program
NRO	National Reconnaissance Office
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
RDT&E	research, development, testing, and evaluation
SCC	Service cryptologic component
SIGINT	signals intelligence
SOTA	SIGINT operational tasking authority
USCG	United States Coast Guard
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USSS	United States SIGINT System
USSOCOM	United States Special Operations Command

*Change 1, 11/19/2010*

USSTRATCOM United States Strategic Command

## PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this Instruction.

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

CSS. An organization that conducts SIGINT collection, processing, analysis, production, and dissemination, and other cryptologic operations as assigned by the DIRNSA/CHCSS. (See Reference (d) for CSS authorities, responsibilities, and functions.)

defense intelligence. Integrated departmental intelligence that covers the broad aspects of national policy and national security and the intelligence relating to capabilities, intentions, and activities of foreign powers, organizations, or persons including any foreign military or military-related situation or activity that is significant to defense policymaking or the planning and conduct of military operations and activities. Defense intelligence includes military, strategic, operational, and tactical intelligence.

DIOCC. The DoD lead organization for planning, integrating, coordinating, directing, synchronizing, and managing full-spectrum defense intelligence capabilities, to include defense collection management and intelligence, surveillance, and reconnaissance.

foreign intelligence. Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

intelligence planning. The intelligence portion of adaptive planning. Its products are the Annex-B/Intelligence Plan (Intelligence Plan of the Combatant Commander's Operations Plan/Concept Plan and the National Intelligence Support Plan).

JIOC. An organization established to create interdependent operational intelligence capabilities at the Combatant Command and operational levels. JIOCs seamlessly integrate all DoD intelligence functions and disciplines and make available all sources of intelligence across the Department of Defense to positively affect U.S. military operations consistent with laws, regulations, and Attorney General-approved procedures.

military intelligence. Information relating to any foreign military or military-related situation or activity significant to military policymaking or the planning and conduct of military operations and activities.

national intelligence. All intelligence, regardless of the source from which derived and including

*Change 1, 11/19/2010*

18

GLOSSARY

~~FOR OFFICIAL USE ONLY~~



information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, or that is determined for the purpose of access to information by the DNI in accordance with section 1.3(a) (1) of Reference (h), to pertain to more than one U.S. Government agency, 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 U.S. national or homeland security.

**NIP.** All programs, projects, and activities of the IC as well as any other programs of the IC designated jointly by the DNI and the head of a United States department or agency or by the President. This term does not include programs, projects, or activities of the Military Departments to acquire intelligence solely for the planning and conduct of tactical military operations by the U.S. Armed Forces.

**operational control.** Direction or exercise of authority over personnel and resources necessary to accomplish the operational and support mission. Operational control may be delegated within a Combatant Command.

**SCC.** Term used to designate, separately or collectively, elements of the U.S. Army, Marine Corps, Navy, Air Force, and Coast Guard assigned to a CSS by the Secretary of Defense for the conduct of cryptologic operations funded by NSA/CSS. The SCC commanders represent the interests of their respective cryptologic forces.

**SIGINT.** A category of intelligence comprising, either individually or in combination, all communications intelligence, electronic intelligence, and foreign instrumentation signal intelligence, however transmitted.

**SIGINT advisory tasking.** The DIRNSA/CHCSS authority to levy tasking against military units, platforms, or other assets that have SIGINT capabilities but whose primary purpose is not SIGINT collection, processing, or other SIGINT-related activities. To exercise this authority, the DIRNSA/CHCSS must:

Have the concurrence of the affected commander;

Not interfere with the primary purpose of the resource or the mission of the command to which it is assigned; and

Provide guidance to ensure the resulting SIGINT product is provided to the designated NSA/CSS office or activity as soon as possible.

**SIGINT operational control.** The DIRNSA/CHCSS authoritative direction of SIGINT activities (assignment of SIGINT missions), including tasking and allocation (SOTA), and the

authoritative prescription of those uniform techniques and standards by which SIGINT information is collected, processed, and reported.

SIGINT operational tasking. The authoritative operational direction and direct levying of SIGINT information needs by a military commander on designated SIGINT resources. These requirements are directive, irrespective of other priorities, and are conditioned only by the capability of those resources to produce such information. Operational tasking includes authority to deploy all or part of the SIGINT resources for which SIGINT operational tasking authority has been delegated.

SIGINT supplemental tasking. Tasking for direct support elements and/or units provided by the DIRNSA, acting as the CHCSS, that may be executed when it does not interfere with the primary purpose of the resource or the mission of the commands to which they are assigned. Also referred to as “supplemental tasking.”

SOTA. The authority to operationally direct and levy SIGINT requirements on designated SIGINT resources. For DoD forces, this includes authority to deploy and redeploy all or part of units with designated SIGINT resources for which SOTA has been delegated and after appropriate Secretary of Defense permissions have been received. SOTA is always documented, usually by letter for STANDING SOTA or by message for TEMPORARY SOTA. These two SOTA categories are defined as:

STANDING. This category is based on long-term needs requiring dedicated, often specialized SIGINT assets and capabilities that are permanently assigned. This type of delegation is negotiated between the DIRNSA/CHCSS and the appropriate Military Service or the USCG.

TEMPORARY. This category is based on direct support needs that can be met by temporarily delegating that portion of SIGINT operational control dealing with directing the tasking and allocation effort of a SIGINT asset. This type of delegation is arranged between the delegated entity and the DIRNSA/CHCSS through Unified Combatant Command channels.

USSS. The unified organization of signals intelligence activities under the direction of the DIRNSA/CHCSS. It consists of the NSA/CSS, the components of the Military Services and the USCG who are authorized to conduct signals intelligence, and such other entities authorized by the Secretary of Defense or the DIRNSA/CHCSS to conduct SIGINT activities.