



Department of Defense

DIRECTIVE

NUMBER 5100.20
January 26, 2010

DA&M

SUBJECT: National Security Agency/Central Security Service (NSA/CSS)

References: See Enclosure 1

1. PURPOSE. Under the authorities vested in the Secretary of Defense by title 10, United States Code (U.S.C.); title 44, U.S.C.; title 50, U.S.C.; Executive Order (E.O.) 12333; and National Security Directive 42 (References (a) through (e), respectively) and pursuant to DoD Directives (DoDDs) 5143.01 and 5144.1 (References (f) and (g)), this Directive reissues DoDD 5100.20 (Reference (h)) to update the mission, organization and management, responsibilities and functions, relationships, authorities, and administration of NSA/CSS, incorporating and cancelling DoDD 5100.23 (Reference (i)). This Directive shall be interpreted consistent with law, policy, and directive, including, as applicable, those related to the Director of National Intelligence (DNI).

2. APPLICABILITY. This Directive applies to OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), 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 in the Department of Defense (hereafter referred to collectively as the "DoD Components").

3. DEFINITIONS. See Glossary.

4. MISSION. The National Security Agency (NSA) is the U.S. Government (USG) lead for cryptology, and its mission encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) activities. The Central Security Service (CSS) conducts SIGINT collection, processing, analysis, production, and dissemination, and other cryptologic operations as assigned by the Director, NSA/Chief, CSS (DIRNSA/CHCSS). NSA/CSS provides SIGINT and IA guidance and assistance to the DoD Components, as well as national customers, pursuant to References (d) and (e). The DIRNSA/CHCSS serves as the principal SIGINT and IA advisor to the Secretary of Defense, the Under Secretary of Defense for Intelligence (USD(I)), the Assistant

Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO), the Chairman of the Joint Chiefs of Staff, the Combatant Commanders, the Secretaries of the Military Departments, and the DNI, as well as other USG officials with regard to these missions and the responsibilities enumerated herein.

5. ORGANIZATION AND MANAGEMENT

a. NSA/CSS is a Defense Agency. The Secretary of Defense exercises authority, direction, and control over NSA/CSS, pursuant to References (a) through (e), Presidential Memorandum (Reference (j)), and other applicable authorities. The USD(I) exercises the authority, direction, and control of the Secretary of Defense over the DIRNSA/CHCSS, pursuant to Reference (f) and the responsibilities and authorities of the Secretary of Defense in References (a), (c), (d), and (e), and in coordination with the ASD(NII)/DoD CIO concerning IA.

b. NSA/CSS is designated a Combat Support Agency of the Department of Defense, pursuant to Reference (a) and Secretary of Defense Memorandum (Reference (k)). NSA/CSS performs combat support activities, pursuant to References (a) and (j), and Secretary of Defense Memorandums (References (k) and (l)), in a manner consistent with DoDD 3000.06 (Reference (m)). These activities are also defined in Acting Chairman of the Joint Chiefs of Staff Memorandum (Reference (n)).

c. NSA/CSS shall consist of a Director, NSA, who also serves as Chief, CSS; a Deputy Director, NSA; and a Deputy Chief of CSS. All military and civilian positions of the NSA/CSS are designated as critical sensitive positions and will be treated as such in connection with investigative, security clearance, and employment matters, pursuant to sections 831-835 of Reference (c).

d. The Service Cryptologic Components (SCCs) of NSA/CSS are composed of those Military Service elements assigned to CSS by the Secretary of Defense in support of the NSA/CSS mission. The SCC commanders are subordinate to the CHCSS for all cryptology matters, and are otherwise subordinate within their respective Military Departments.

e. NSA/CSS is also an element of the Intelligence Community (IC) subject to the oversight of the DNI, pursuant to References (c) and (d). The DNI provides objectives, priorities, and guidance for, determines requirements and the budget of, and exercises execution, transfer, and reprogramming authorities over the National Intelligence Program (NIP) portion of the NSA/CSS budget. The DNI also exercises National Intelligence tasking and oversight; certain authorities for personnel, acquisition management, security, information technology, education and training; oversight of intelligence coordination with foreign governments and international organizations; and other applicable authorities over NSA/CSS, pursuant to References (c) and (d). The DIRNSA/CHCSS shall keep the USD(I) fully informed of all National Intelligence activities undertaken by NSA/CSS that are tasked by the DNI. The DIRNSA/CHCSS shall assist the Secretary of Defense and the DNI in their respective responsibilities to manage, develop, and ensure implementation of policies, principles, standards, and guidelines for the security of information systems supporting the operations under their respective control, as well as

supporting the operations of other USG departments and agencies with national security information.

6. RESPONSIBILITIES AND FUNCTIONS. The DIRNSA/CHCSS, under the authority, direction, and control of the USD(I), serves as the principal advisor to the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Combatant Commanders on SIGINT, pursuant to National Security Council Intelligence Directive Number 6 (Reference (o)). The DIRNSA/CHCSS shall also advise the DNI and the Director of Defense Intelligence (DDI) – as established in the Secretary of Defense and DNI Memorandum of Agreement (Reference (p)) – on all matters under the purview of the DNI concerning SIGINT and serves as the SIGINT Functional Manager, pursuant to Reference (d). The DDI will advise the DNI on critical deficiencies and strengths in SIGINT-related Defense Intelligence capabilities after consultation with the DIRNSA/CHCSS, and provide assessments on the effect of such deficiencies and strengths in meeting National Intelligence objectives. In the exercise of these responsibilities, the DIRNSA/CHCSS shall plan, organize, direct, and manage NSA/CSS and all assigned resources to provide peacetime, contingency, crisis, and combat SIGINT and IA support to the operational Armed Forces of the United States. The DIRNSA/CHCSS shall develop and manage those Military Intelligence Program (MIP) resources and capabilities under the purview of NSA/CSS, pursuant to DoDD 5205.12 (Reference (q)). The DIRNSA/CHCSS shall contribute to the security of critical USG classified operations and information through appropriate IA measures. The DIRNSA/CHCSS shall operate security programs to protect people, facilities, and information. The DIRNSA/CHCSS shall conduct counterintelligence activities as assigned by DoDD O-5240.02 (Reference (r)). Additionally, the DIRNSA/CHCSS shall plan and provide for survival, recovery, and reconstitution of NSA/CSS mission-essential functions, pursuant to Reference (d) and DoDD 3020.26 (Reference (s)). The DIRNSA/CHCSS shall provide for, operate, and maintain the Critical Information Communications (CRITICOMM) System and operations, pursuant to Director of Central Intelligence Directive (DCID) 7/4 and DoDD C-5100.19E (References (t) and (u)). The DIRNSA/CHCSS shall:

a. SIGINT

(1) Collect (including through clandestine means), process, analyze, produce, and disseminate SIGINT information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions, pursuant to Reference (d).

(2) Provide SIGINT support for the conduct of military operations, pursuant to tasking, priorities, and standards of timeliness assigned by the Secretary of Defense. If provision of such support requires use of national collection systems, these systems will be tasked within existing guidance from the DNI, pursuant to Reference (d). No other organization within the Department of Defense shall engage in SIGINT activities, except when directed or delegated by the Secretary of Defense or the DIRNSA/CHCSS after coordination with the DNI, or as otherwise provided for in Reference (o).

(3) Establish and operate an effective, unified organization for SIGINT activities, including executing any SIGINT-related functions the Secretary of Defense so directs.

(4) Protect intelligence sources, methods, and activities from unauthorized disclosure, pursuant to E.O. 12958 (Reference (v)) and guidance received from the DNI, pursuant to References (c) and (d).

(5) Develop rules, regulations, and standards governing the classification and declassification of SIGINT, pursuant to References (d) and (v).

(6) Prescribe security regulations covering operating practices, including the transmission, handling, and distribution of SIGINT material within and between elements under DIRNSA/CHCSS control, and exercise the necessary supervisory control to ensure compliance with these regulations, pursuant to Reference (d).

(7) Exercise SIGINT operational control and establish policies and procedures for departments and agencies to follow when appropriately performing SIGINT activities in order for the SIGINT mission of the United States to be accomplished in the most efficient and effective manner. In the case of service mobile SIGINT platforms, systems, or assets used to collect SIGINT, the DIRNSA/CHCSS shall state movement requirements through appropriate channels to the military commanders, who shall retain responsibility for operational command of the platforms.

(8) Provide technical guidance and assistance to all USG SIGINT or SIGINT-related operations.

(9) Conduct SIGINT research, development, and systems design, and perform SIGINT-related testing and evaluation. Provide expertise to SIGINT-related research, development, and testing and evaluation conducted by the DoD Components.

(10) Conduct modeling and simulation activities related to SIGINT. Advise and coordinate on all SIGINT modeling and simulation activities within or on behalf of the Heads of the DoD Components, pursuant to DoDD 5000.59 (Reference (w)).

(11) Co-manage, with the Director, Defense Intelligence Agency (DIA), and support, as appropriate, the activities of the Defense Special Missile and Aerospace Center, pursuant to DoD Instruction (DoDI) S-5100.43 (Reference (x)).

(12) Provide support to national level forums that review SIGINT strategies and matters of international policy that may affect SIGINT equities, and assess future SIGINT capabilities on behalf of the Secretary of Defense and the DNI.

b. IA

(1) Serve as the National Manager for National Security Telecommunications and Information Systems Security as provided for by References (b), (d), and (e). In this capacity, the DIRNSA/CHCSS is responsible to the Secretary of Defense for the security of National Security Systems (NSS) and to the DNI for those NSS that also qualify as intelligence systems.

(2) Provide IA support to the Department of Defense, pursuant to DoDD 8500.01E (Reference (y)).

(3) Prescribe minimum standards, methods, and procedures for protecting cryptographic and other sensitive communications security (COMSEC), information security (INFOSEC), and other IA materials, techniques, and information to be employed by all NSS owners.

(4) Review and approve all COMSEC, INFOSEC and, in conjunction with other DoD Components, other IA standards, techniques, systems, and equipment for applications within NSS. Coordinate with the DNI for the safeguarding of national security information within the NSS of IC elements. Assess the overall NSS security posture and disseminate information on threats to, and vulnerabilities of, those systems.

(5) Conduct, approve, or endorse COMSEC, INFOSEC, and research and development activities supportive of the NSA/CSS national mission. Coordinate research and development activities with the Director, Defense Research and Engineering, pursuant to Reference (y).

(6) Enter into agreements for the procurement of COMSEC, INFOSEC, or other IA materials and equipment, and provide or coordinate the provision of such materials and equipment to other USG departments and agencies, and, where appropriate, to USG contractors, foreign governments, and private organizations.

(7) Assist other USG departments and agencies in developing effective telecommunications and computer systems architectures necessary to satisfy COMSEC, INFOSEC, or other IA requirements for their NSS, and provide technical assistance and services upon request for their non-national security systems, pursuant to Reference (b).

(8) Coordinate with the National Institute of Standards and Technology, pursuant to sections 3541-3549 of Reference (b).

(9) Coordinate with the Committee on National Security Systems (CNSS) to ensure the development of necessary security architectures, and to approve minimum NSS security standards and doctrine.

(10) Provide personnel, facilities, and administrative support to the CNSS, pursuant to Reference (e).

(11) Formulate and disseminate procedures for integrated material management of COMSEC and INFOSEC equipment, and maintain a process for the disposal of unserviceable, obsolete, or excess equipment.

(12) Manage, design, evaluate, and operate critical functions of a key management or enterprise security management infrastructure, as required, to support COMSEC, INFOSEC, or other IA equipment or related products, pursuant to References (b), (d), (e), and DoDI 8523.01 (Reference (z)).

(13) Operate and/or sustain a capability to provide microelectronic products and services responsive to the SIGINT and IA requirements of the NSA/CSS enterprise, and other sensitive activities conducted by other USG departments and agencies.

(14) Provide attack sensing and warning support to the Commander, U.S. Strategic Command (USSTRATCOM) and to the Heads of the other DoD Components, pursuant to DoDD O-8530.1 (Reference (aa)).

(15) Serve as the focal point for delivery of unique, tailored, and time-critical IA support to external customers, pursuant to guidance provided by the ASD(NII)/DoD CIO in Reference (z).

(16) Provide COMSEC monitoring services to the Department of Defense and other USG departments and agencies, pursuant to DoDI 8560.01 (Reference (ab)).

(17) Develop and maintain a capability to execute national-level COMSEC monitoring and IA readiness testing efforts for employment in single Military Service, joint, and national-level exercises, operations, and other activities as directed, pursuant to Reference (ab).

(18) Conduct computer network defense (CND) activities, and support DoD organization, planning, assessment, training, and conduct of CND, pursuant to Reference (aa).

(19) Provide cyber security assistance services, coordination, and information to USG departments and agencies, as requested.

c. Operations Security (OPSEC). Act as the Federal Executive Agent for Interagency OPSEC training, pursuant to National Security Decision Directive 298 and DoDD 5205.02 (References (ac) and (ad)), and in that capacity maintain an interagency OPSEC support staff with a core expertise to assist USG departments and agencies, as needed, in establishing OPSEC programs, conducting surveys, providing services, and developing and providing interagency training and awareness courses and products.

d. Cryptologic Program Management

(1) Serve as the Program Manager (PM) for the Consolidated Cryptologic Program (CCP); develop the CCP as a portion of the NIP; participate in the NIP development process; and oversee execution of funds appropriated for the CCP.

(2) Prepare and submit NSA/CSS program and budget input for the CCP to the DNI and USD(I), pursuant to DNI guidance, as well as prepare and submit the NSA/CSS program and budget input for the NSA/CSS MIP to the USD(I) and DNI, pursuant to USD(I) guidance. Serve as the Component Manager for the NSA/CSS MIP, pursuant to Reference (q).

(3) Serve as PM for the NSA/CSS portion of the Information Systems Security Program (ISSP); formulate the ISSP; review the proposed COMSEC, INFOSEC, and other IA programs

and budgets for USG departments and agencies; and prepare consolidated recommendations for submission to the Secretary of Defense through the ASD(NII)/DoD CIO.

(4) Serve as the ASD(NII)/DoD CIO Domain Agent for IA, manage the global information grid IA portfolio, consistent with the processes and procedures specified in DoDI 8115.02 (Reference (ae)), and make IA portfolio investment recommendations to the ASD(NII)/DoD CIO to ensure the efficient and effective delivery of capabilities to the warfighter and to maximize return on investment to the enterprise.

e. International Engagement

(1) Conduct liaison with foreign nations or international organizations regarding SIGINT activities, with the authority of the Secretary of Defense and the DNI, as appropriate, pursuant to Reference (d) and DCID 5/5P (Reference (af)); and IA activities with the authority of the Secretary of Defense, pursuant to References (d) and (e), and with the authority of the DNI, pursuant to Reference (d). As appropriate, coordinate SIGINT and IA agreements and arrangements with other affected USG departments and agencies.

(2) Provide technical advice and support to cryptologic arrangements with foreign governments and international organizations, and conduct, as authorized, cryptologic exchanges, pursuant to References (a), (c), (d), and (e).

(3) Leverage cryptologic capabilities of foreign partners with whom NSA/CSS has an established cryptologic relationship or as requested by the Secretary of Defense or DNI.

(4) Exercise authority and responsibility for disclosing and releasing classified military information to foreign governments, allies, and coalition partners, while providing appropriate policy guidance and training to personnel exercising foreign disclosure duties, pursuant to DoDD 5230.11 and DoDD 5530.3 (References (ag) and (ah)).

f. Cryptologic Training and Education

(1) Provide guidance, as directed by the USD(I), to the Secretaries of the Military Departments and the Commandant of the United States Coast Guard to effect and ensure sound and adequate military and civilian cryptologic career development and training programs; develop cryptologic knowledge and skill standards; and conduct or otherwise provide for necessary specialized and advanced cryptologic training, pursuant to DoDI 3305.09 (Reference (ai)).

(2) Provide linguistic and other training for cryptologic personnel as outlined in Public Law 86-36 (Reference (aj)).

(3) Maintain and operate the National Cryptologic School, pursuant to Reference (ai).

g. Critical Information Reporting and Handling

(1) Exercise authority and responsibility for the reporting and handling of critical information, pursuant to References (d), (t), and (u).

(2) Provide for, manage, and maintain CRITICOMM messaging and cryptographic resources and operations.

(3) Establish, in coordination with the Chairman of the Joint Chiefs of Staff, the Heads of the other DoD Components, and the DNI, procedures for reporting and handling critical information within the CRITICOMM System to ensure fastest delivery possible.

(4) Provide adequate critical information (CRITIC) training resources, and perform regular joint training exercises of the CRITICOMM System.

h. Additional Activities. Perform those additional activities for the Department of Defense and the IC, and such other duties as may be directed by the President of the United States, the Secretary or Deputy Secretary of Defense, the USD(I), the ASD(NII)/DoD CIO, or the DNI.

(1) Develop global network awareness; characterize and report threats to networks to the Department of Homeland Security, the National Cyber Security Center, and other USG cybersecurity and incident reporting centers.

(2) Promote cooperation between NSA/CSS and USSTRATCOM, Joint Task Force-Global Network Operations, with regard to CND; and between NSA/CSS and USSTRATCOM, Joint Functional Component Command for Network Warfare (JFCC-NW), with regard to computer network attack activities.

(3) Serve as Commander, JFCC-NW.

(4) Serve as the Executive Secretary for deconfliction processes for computer network attack and exploitation activities as specified by Memorandum of Agreement among the Department of Defense, the Department of Justice, and other members of the IC (Reference (ak)).

7. RELATIONSHIPS

a. The DIRNSA/CHCSS shall:

(1) Serve as the Functional Manager for SIGINT, pursuant to Reference (d).

(2) Maintain communication with other IC elements, pursuant to References (c) and (d), and other applicable authorities.

(3) Work with the Combatant Commanders to deconflict selected sensitive SIGINT and non-SIGINT operations.

(4) Provide support to the Defense Intelligence Operations Coordination Center (DIOCC) and Combatant Command-level and operational-level centers and respond to validated DoD information needs, pursuant to Defense Intelligence Operations Coordination Center Execute Order (Reference (al)).

(a) Inform the DIOCC and the respective Joint Intelligence Operations Centers of NSA/CSS activities occurring in each Combatant Command area of responsibility, pursuant to Secretary of Defense Memorandum (Reference (am)).

(b) Keep the DIOCC fully informed of the state of readiness of NSA/CSS to meet national and military SIGINT requirements, to include related Global Force Management issues.

(5) Participate, as appropriate, in the Secretary of Defense Biennial Review of Defense Agencies and DoD Field Activities in coordination with the Director of Administration and Management (DA&M).

(6) Notify the USD(I) and the General Counsel of the Department of Defense (GC, DoD), within 90 days of the issuance date when the DIRNSA/CHCSS believes a DoD issuance would damage, limit, or seriously inhibit NSA/CSS from performing its missions.

(7) Support the Combatant Commanders and the Secretaries of the Military Departments, as appropriate.

(8) Coordinate with other USG departments and agencies to maintain the capability to rapidly receive and disseminate CRITIC messages.

(9) Use existing systems, facilities, and services of the Department of Defense and other USG departments and agencies, when possible, to avoid duplication and to achieve maximum efficiency and economy, as well as preserve the capability of assigned facilities and other assets to accomplish the NSA/CSS mission.

(10) Conduct all NSA/CSS activities and report issues or activities that raise questions of legality or propriety to the USD(I), the Inspector General of the Department of Defense, the Assistant to the Secretary of Defense for Intelligence Oversight, and, as appropriate, the GC, DoD, pursuant to DoDD 5240.01 (Reference (an)), DoD Regulation 5240.1-R (Reference (ao)) and appropriate controls and standards of conduct.

b. The Chairman of the Joint Chiefs of Staff shall review and assess NSA/CSS responsiveness and readiness to support operating forces in the event of war or threats to national security, pursuant to References (a) and (m).

c. The Directors of DIA, the National Geospatial-Intelligence Agency, and the National Reconnaissance Office, under the authority, direction, and control of the USD(I), shall provide expertise, capabilities, and all available data and information necessary for the DIRNSA/CHCSS to perform the responsibilities and functions prescribed herein, within existing resources.

d. The ASD(NII)/DoD CIO shall, in consultation and coordination with the USD(I), provide policy guidance to the DIRNSA/CHCSS regarding network operations and IA matters, pursuant to Reference (g).

e. The Heads of the DoD Components shall:

(1) Provide assistance, support, data, and information, in their respective fields of responsibility and within available resources, to the DIRNSA/CHCSS to carry out functions as prescribed herein.

(2) Comply with taskings from the DIRNSA/CHCSS, pursuant to this Directive.

(3) Coordinate with the DIRNSA/CHCSS on all matters concerning the mission, responsibilities, functions, and operations of the NSA/CSS.

f. The Director, Defense Information Systems Agency, under the authority, direction, and control of the ASD(NII)/DoD CIO, shall coordinate with the DIRNSA/CHCSS and the Secretaries of the Military Departments to develop strategic, tactical, and interoperable secure communications architectures, pursuant to Reference (z).

g. The Secretaries of the Military Departments and the Commandant of the U.S. Coast Guard shall:

(1) Enter into agreements with NSA/CSS to provide facilities, systems, and services in support of NSA/CSS activities in the interest of maximum efficiency and economy within the Department of Defense and the U.S. Coast Guard, when practicable.

(2) Assign military personnel, including U.S. Coast Guard, to NSA/CSS, pursuant to approved Joint Manpower Program authorizations as prescribed by OSD, the Chairman of the Joint Chiefs of Staff, and the Commandant of the U.S. Coast Guard.

(3) Designate an organization within each respective Military Service, including the U.S. Coast Guard, as an SCC. The designated organization shall serve as the primary Service authority for all operations, programming, budgeting, training, personnel, policy, doctrine, and foreign relationships for cryptologic activities. The SCC will also have administrative and logistical responsibility for the Military Service or U.S. Coast Guard cryptologic workforce assigned to missions funded by NSA/CSS.

(4) Assign, after consulting with the DIRNSA/CHCSS, the Commander/Chief of their SCC who is normally of at least one-star rank (or equal civilian grade). The Commander/Chief of the SCC shall be subordinate to the CHCSS for all cryptologic matters.

(5) Provide personnel who have been trained to Cryptologic Training System standards, pursuant to Reference (ai) and fully cleared in accordance with DIRNSA/CHCSS standards, for assignment across the NSA/CSS enterprise to include standing task forces.

(6) Provide their NSS plans, programs, and budgets to the DIRNSA/CHCSS for review in his or her capacity as the National Manager for NSS, pursuant to Reference (e).

8. AUTHORITIES. The DIRNSA/CHCSS is hereby delegated authority to:

a. Communicate directly with the Heads of the DoD Components, as necessary, to carry out assigned responsibilities and functions, including requests for advice and assistance. Communications to the Military Departments shall be transmitted through the Secretaries of the Military Departments, the Commandant of the Coast Guard, their designees, or as otherwise provided in law or as 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.

b. Communicate with other Government officials, representatives of the Legislative Branch, members of the public, and representatives of foreign governments or other entities, as appropriate, in carrying out assigned responsibilities and functions. Communications with representatives of the Legislative Branch will be coordinated with the Assistant Secretary of Defense for Legislative Affairs or the Under Secretary of Defense (Comptroller)/Chief Financial Officer of the Department of Defense, as applicable, and be consistent with the DoD Legislative Program. Those issues which fall under the purview of the DNI will be coordinated with the DNI.

c. Obtain reports, information, advice, and assistance, pursuant to DoDD 4630.05 (Reference (ap)) and DoDI 8910.01 (Reference (aq)), as necessary, to carry out assigned responsibilities and functions.

d. Provide for, manage, operate, and maintain the CRITICOMM System, including reporting and handling critical information through that system.

e. Establish and maintain relationships with foreign governments and other entities, consistent with References (a), (c), (d), (e), and (af).

f. Publish guidance to the DoD Components in carrying out assigned responsibilities prescribed herein in accordance with the authorities contained in Enclosure 2.

g. Authorize another USG department or agency to engage in SIGINT activities in coordination with the DNI. This authority may not be further delegated and actions taken, pursuant to this authority, shall be summarized periodically and reported to the Secretary of Defense.

h. Disseminate SIGINT within the IC, pursuant to paragraph 2.3 of Reference (d) and procedures established by the DNI in coordination with the Secretary of Defense and approved by the Attorney General.

(1) Dissemination to IC elements of SIGINT that may contain identifying information of U.S. persons shall be done, pursuant to procedures established by the DNI and approved by the Attorney General, or pursuant to orders of the Foreign Intelligence Surveillance Court in response to applications from the IC and approved by the Attorney General.

(2) Dissemination of SIGINT may be made to the intelligence elements of the Military Services, intelligence elements within DoD Components conducting computer network operations, and other IC elements, as required.

- i. Exercise the administrative authorities contained in Enclosure 2.

9. ADMINISTRATION

a. The DIRNSA/CHCSS shall be recommended for appointment by the Secretary of Defense only after obtaining the concurrence of the DNI, as provided for in References (a), (c), and (d). The DIRNSA/CHCSS shall be a commissioned officer in the Military Services, on active or reactivated status, and shall enjoy not less than three-star rank during the period of incumbency, pursuant to Reference (o).

b. NSA shall also have a Deputy Director who shall be a career civilian with cryptologic experience, pursuant to Reference (o). The Deputy Director shall be designated by the Secretary of Defense, in consultation with the USD(I) and the DNI, and approved by the President of the United States.


c. The Deputy Chief of the CSS shall be a commissioned officer in the Military Services not less than a two-star rank, who will not normally be selected from the same Military Service as the DIRNSA/CHCSS, and will be approved by the Secretary of Defense.

d. The DIRNSA/CHCSS shall be authorized such personnel, facilities, funds, and other resources as the Secretary of Defense or the DNI, as applicable, deems appropriate including facilities, services, and other support from the Military Departments. The DIRNSA/CHCSS may obtain personnel, administrative, and contracting support from the Heads of the other DoD Components, the Director of the Central Intelligence Agency, the Secretary of Homeland Security, and/or the DNI, to the extent permitted by law.

e. The DIRNSA/CHCSS is authorized to conduct such administrative and technical support activities within and outside the United States as are necessary to perform the functions described in sections 1.4 and 1.7(c) of Reference (d), References (e) and (af) and, as otherwise provided by law and E.O., as well as guidance from the President, the Secretary of Defense, or the DNI.

10. RELEASABILITY. UNLIMITED. This Directive is approved for public release and may be obtained on the Internet at the DoD Issuances Web Site: <http://www.dtic.mil/whs/directives>.

11. EFFECTIVE DATE. This Directive is effective immediately.



Robert M. Gates
Secretary of Defense

Enclosures

1. References
 2. Delegations of Authority
- Glossary

ENCLOSURE 1

REFERENCES

- (a) Title 10, United States Code
- (b) Title 44, United States Code
- (c) Title 50, United States Code
- (d) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
- (e) National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information," July 5, 1990¹
- (f) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),
November 23, 2005
- (g) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
- (h) DoD Directive 5100.20, "The National Security Agency and the Central Security Service," December 23, 1971 (hereby canceled)
- (i) DoD Directive 5100.23, "Administrative Arrangements for the National Security Agency," May 17, 1967 (hereby canceled)
- (j) Presidential Memorandum to the Secretary of State and the Secretary of Defense, "Communications Intelligence Activities," October 24, 1952²
- (k) Secretary of Defense Memorandum for the Chairman of the Joint Chiefs of Staff and DIRNSA, "Policy and Procedures Related to NSA's Role as a Combat Support Agency," June 21, 1988³
- (l) Secretary of Defense Memorandum for the Chairman of the Joint Chiefs of Staff and DIRNSA, "Combat Support Functions of the National Security Agency/Central Security Service," November 10, 1988³
- (m) DoD Directive 3000.06, "Combat Support Agencies," July 10, 2007
- (n) Acting Chairman of the Joint Chiefs of Staff Memorandum for the Secretary of Defense, "Combat Support Functions of the National Security Agency/Central Security Service," October 18, 1988⁴
- (o) National Security Council Intelligence Directive No. 6, "Signals Intelligence," February 17, 1972
- (p) Memorandum of Agreement between the Secretary of Defense and the Director of National Intelligence on the Director of Defense Intelligence, May 21, 2007²
- (q) DoD Directive 5205.12, "Military Intelligence Program (MIP)," November 14, 2008
- (r) DoD Directive O-5240.02, "Counterintelligence," December 20, 2007⁵
- (s) DoD Directive 3020.26, "Department of Defense Continuity Programs," January 9, 2009
- (t) Director of Central Intelligence Directive 7/4: "Critical Information (CRITIC)," January 2, 2001⁶

¹ Available on SIPRNET at http://www.iad.nsa.smil.mil/resources/library/natl_pols_dirs_orders_section/index.cfm.

² Copies may be requested from the Office of the USD(I) at USDI.Pubs@osd.mil.

³ Available to authorized users at https://usdi.dtic.mil/usdi_docs/keyref/usdi_keyref.cfm.

⁴ For official use only; copies available from the Office of the USD(I) at USDI.pubs@osd.mil.

⁵ For official use only; copies available at the DoD Issuance SIPRNET site: <http://www.dtic.smil.mil/whs/directives>.

⁶ Copies are available on SIPRNET at http://capco.dssc.sgov.gov/dcids_home.htm.

- (u) DoD Directive C-5100.19E, "Critical Information Communications (CRITICOMM) System (U)," June 10, 2008
- (v) Executive Order 12958, "Classified National Security Information," April 17, 1995, as amended
- (w) DoD Directive 5000.59, "DoD Modeling and Simulation (M&S) Management," August 8, 2007
- (x) DoD Instruction S-5100.43, "Defense Special Missile and Aerospace Center (DEFSMAC)," September 24, 2008
- (y) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
- (z) DoD Instruction 8523.01, "Communications Security (COMSEC)," April 22, 2008
- (aa) DoD Directive O-8530.1, "Computer Network Defense (CND)," January 8, 2001⁷
- (ab) DoD Instruction 8560.01, "Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing," October 9, 2007
- (ac) National Security Decision Directive No. 298, "National Operations Security Program," January 22, 1988
- (ad) DoD Directive 5205.02, "DoD Operations Security (OPSEC) Program," March 6, 2006
- (ae) DoD Instruction 8115.02, "Information Technology Portfolio Management Implementation," October 30, 2006
- (af) Director of Central Intelligence Directive 5/5P, "Conduct of Liaison with Foreign Governments and the Release of U.S. SIGINT to Foreign Governments," May 17, 1983⁶
- (ag) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
- (ah) DoD Directive 5530.3, "International Agreements," June 11, 1987
- (ai) DoD Instruction 3305.09, "DoD Cryptologic Training," December 22, 2006
- (aj) Public Law 86-36, "National Security Agency Act of 1959," as amended
- (ak) Memorandum of Agreement among the Department of Defense, the Department of Justice, and the Intelligence Community Regarding Computer Network Attack and Exploitation Activities, May 9, 2007²
- (al) Defense Intelligence Operations Coordination Center Execute Order, December 4, 2007⁸
- (am) Secretary of Defense Memorandum, "Defense Intelligence Operations Coordination Center Establishment Directive," October 1, 2007
- (an) DoD Directive 5240.01, "DoD Intelligence Activities," August 27, 2007
- (ao) DoD Regulation 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 7, 1982
- (ap) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 5, 2004
- (aq) DoD Instruction 8910.01, "Information Collection and Reporting," March 6, 2007

⁷ For official use only; a copy can be requested by authorized users from the Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer at 703-614-7323.

⁸ For official use only; a copy can be requested from the J-2/Joint Staff at 703-614-7816.

ENCLOSURE 2

DELEGATIONS OF AUTHORITY

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 and issuances, the DIRNSA/CHCSS or in the absence of the DIRNSA/CHCSS, the person acting for the DIRNSA/CHCSS, is hereby delegated authority, as required, in the administration of NSA/CSS missions and operations as follows:

a. Human Resources

(1) Exercise the authority vested in the Secretary of Defense according to sections 301, 302(b), 3101, and 5107 of title 5, U.S.C., and Chapter 83 of title 10, U.S.C., as amended, on the employment, direction, and general administration of NSA/CSS civilian personnel.

(2) Fix rates of pay for wage-rate employees exempted from the Classification Act of 1949 according to section 5102 of title 5, U.S.C., on the basis of rates established under the Federal Wage System. In fixing such rates, the DIRNSA/CHCSS shall follow the wage schedule established by the DoD Wage Fixing Authority.

(3) Pursuant to the authority vested in the Secretary of Defense under section 1609 of title 10, U.S.C., terminate the employment of NSA/CSS employees. This authority may NOT be further delegated.

(4) Administer oaths of office to those entering the Executive Branch of the Federal Government or any other oath required by law in connection with employment therein, pursuant to section 2903 of title 5, U.S.C., and designate in writing, as may be necessary, officers and employees of NSA/CSS to perform this function.

(5) Carry out delegations regarding the Defense Civilian Intelligence Personnel System (DCIPS) as prescribed in DoDD 1400.35.

(6) Prescribe, as conditions of employment, that NSA employees must serve any place in the world as the needs of the Agency dictate and must forego personal unofficial travel when the DIRNSA determines that travel in the proposed area would constitute a hazard to national security.

(7) Establish an NSA/CSS Incentive Awards Board and pay cash awards to, and incur necessary expenses for, the honorary recognition of USG civilian employees whose suggestions, inventions, superior accomplishments, or other personal efforts, including special acts or services, benefit NSA/CSS, pursuant to section 4503 of title 5, U.S.C., Office of Personnel Management (OPM) regulations, and DoDI 1400.25.

(8) Establish a joint military recognition program, pursuant to DoD 1348.33-M.

(9) Act as agent for the collection and payment of employment taxes imposed by appropriate statutes.

(10) As necessary, use advisory committees and employ temporary or intermittent experts or consultants, as approved by the Secretary of Defense or the DA&M, in support of NSA/CSS functions, consistent with section 173 of title 10, U.S.C.; section 3109(b) of title 5, U.S.C.; Federal Advisory Committee Act, title 5, U.S.C. Appendix 2; and DoDI 5105.04 and DoDD 5105.18.

(11) Authorize and approve:

(a) Temporary duty travel for military personnel assigned or detailed to NSA/CSS, pursuant to Joint Federal Travel Regulations, Volume 1, "Uniformed Service Members."

(b) Travel for NSA/CSS civilian employees, pursuant to Joint Travel Regulations, Volume 2, "DoD Civilian Personnel."

(c) Invitational travel to non-DoD personnel whose consultative, advisory, or other highly specialized technical services are required in a capacity that is directly related to or in connection with NSA/CSS activities, pursuant to section 5703 of title 5, U.S.C., and Joint Travel Regulations, Volume 2, "DoD Civilian Personnel."

(d) Overtime work for NSA/CSS civilian employees, pursuant to chapter 55, subchapter V of title 5, U.S.C., and applicable OPM regulations.

(e) Funds available for travel by military personnel assigned or detailed to NSA/CSS for expenses incident to attendance at meetings of technical, scientific, professional, or other similar organizations in such instances when the approval of the Secretary of Defense, or designee, is required by section 412 of title 37, U.S.C., and sections 4110 and 4111 of title 5, U.S.C.

b. Security

(1) Pursuant to E.O.s 10450, 12333, 12958, 12968, and 13467; DoDD 5200.02; DoDIs 5200.01 and 5210.45; and DoD 5200.2-R and, as applicable, DCIDs and Intelligence Community Directives (ICD) (such as ICD 704), and DNI regulations, as appropriate (copies of DCIDs and ICDs are available to SIPRNET users at http://capco.dssc.gov/dcids_home.htm):

(a) Authorize persons to be provisionally employed before the completion of a full field investigation, provided such persons are not given access to sensitive cryptologic information while so employed, in accordance with section 302(a) of Public Law 88-290. In an exceptional case in which the DIRNSA/CHCSS makes a determination in writing that his or her action is necessary or advisable in the national interest, the DIRNSA/CHCSS may authorize the employment, detail, or assignment of any person to NSA/CSS and may grant any such person access to sensitive cryptologic information; these actions shall be on a temporary basis pending the completion of a full field investigation. In these cases, priority shall be given to the full field

investigation of these individuals, in accordance with section 302(a) of Public Law 88-290 and DoDI 5210.45.

(b) Initiate appropriate full field investigations and, if necessary, in the interest of national security, suspend security clearances for personnel cleared by NSA, or deny all access for personnel assigned or detailed to NSA/CSS. Any actions under this paragraph shall be taken in accordance with procedures prescribed in DoDD 5200.02.

(c) Provide for and establish boards of appraisal to assist the DIRNSA/CHCSS in discharging his or her personnel security responsibilities to appoint the members of such boards and to make the determination that a person's employment, detail, assignment, or access to classified information is or is not in the national interest, pursuant to sections 831-835 of title 50, U.S.C., and the provisions of E.O. 12968, DoDD 5210.48, DoDI 5210.45, and all applicable ICDs.

(d) Promulgate the necessary security policies for the physical protection of property and places under the jurisdiction of the DIRNSA/CHCSS, including those in industry wherein NSA/CSS Sensitive Compartmented Information (SCI) resides, pursuant to E.O. 12333, DoDI 5200.01, and applicable DNI guidance. Promulgate regulations governing the granting or denial of industrial clearances for access to sensitive cryptologic information and regulate physical security in industry or NSA/CSS-sponsored contracts for sensitive cryptologic materials.

(e) Grant, suspend, deny, or revoke security clearances of individuals under the cognizance of the DIRNSA/CHCSS. Individuals subject to denial or revocation are entitled to review and appeal procedures, pursuant to E.O. 12968 and ICD 704. Notice to an NSA/CSS employee of the determination to revoke access shall include notice to remove from employment, pursuant to Public Law 88-290 and DoDI 5210.45.

(f) Determine initial and continued SCI access eligibility for all individuals under the cognizance of the DIRNSA/CHCSS, pursuant to E.O. 12333 and ICD 704. Clear NSA/CSS personnel and such other individuals as may be appropriate for access to classified DoD material and information, pursuant to DoDD 5200.02 and DoDI 5210.45.

(2) Protect the security of NSA/CSS installations, activities, property, information, and personnel by appropriate means, including the publication of necessary security regulations.

(3) Conduct personnel security investigations relating to civilians, contractors, members of the Armed Forces, and others with similar affiliations with NSA/CSS who are employed in, or assigned to, NSA/CSS, pursuant to E.O.s 12333 and 13467; DCID 6/1; ICD 704; and DoDI 5210.45. Conduct polygraph examinations in accordance with DoDD 5210.48, DoDI 5210.45, and all applicable ICDs.

(4) Impose, when necessary, special requirements on the classification, declassification, marking, reproduction, distribution, accounting, and protection of and access to classified cryptographic information as the designee of the Secretary of Defense, pursuant to DoDI 5200.01.

(5) Establish, direct, and administer all aspects of the NSA/CSS security program for the protection of SCI, including all necessary coordination and implementation of DNI security policy, pursuant to E.O. 12333, DCID 6/1, and DoDI 5200.01.

c. Counterintelligence (CI). Maintain an organic CI program that identifies vulnerabilities and recommends countermeasures to mitigate threats posed to NSA/CSS operations by opposition foreign intelligence services, and resolves matters of internal CI concern.

d. Records

(1) Maintain an official seal and attest to the authenticity of official NSA/CSS records under that seal.

(2) Develop, establish, and maintain an active and continuing Records Management Program, pursuant to section 3102 of title 44, U.S.C., and DoDD 5015.2.

e. Publications

(1) Authorize the publication of advertisements, notices, or proposals in newspapers, magazines, or other public media, as required, for the effective administration and operation of NSA/CSS, consistent with section 3702 of title 44, U.S.C.

(2) Establish and maintain, for the functions assigned, an appropriate publications system for common supply and service regulations, instructions, and reference documents, and changes thereto, pursuant to DoDI 5025.01.

f. Acquisition/Procurement, Financial Management, and Property

(1) Enter into support and service agreements with the Military Departments, other DoD Components, and other USG departments and agencies, as required, for the effective performance of NSA/CSS responsibilities and functions.

(2) Enter into and administer contracts, directly or through a Military Department, DoD contract administration services component, or other USG departments and agencies, as appropriate, for supplies, equipment, and services required to accomplish the NSA/CSS mission. To the extent that any law or E.O. specifically limits such authority to persons at the Secretarial level of a Military Department, such authority shall be exercised by the appropriate Under Secretary of Defense or Assistant Secretary of Defense.

(3) Use the Government-Wide Commercial Purchase Card for making appropriate purchases of material and services, other than personal services, for NSA/CSS when it is determined to be more advantageous and consistent with the best interests of the Government.

(4) Lease non-excess property under the control of NSA/CSS, under terms that will promote the National Defense or that will be in the public interest, under section 2667a of title 10, U.S.C.

(5) Serve as the Milestone Decision Authority (MDA) for NSA/CSS programs funded wholly or with the majority of funds available from the Department of Defense, including the MIP, pursuant to DoDI 5000.02, and the Memorandum of Agreement between the DNI and the Secretary of Defense, "Management of Acquisition Programs Executed at the Department of Defense Intelligence Community Elements," for less than Acquisition Category (ACAT) ID, and serve as the MDA for less than ACAT IAM programs, when appropriately delegated by the Secretary of Defense, pursuant to DoDI 5000.02. The DIRNSA/CHCSS shall exercise such delegated MDA, pursuant to delegation instructions and applicable procedures as directed by the Secretary of Defense.

(6) Serve as MDA for major systems funded wholly or in majority by the NIP, pursuant to section 403(9) of title 41, U.S.C. and section 403-1 of title 50, U.S.C., when appropriately delegated jointly by the Secretary of Defense and the DNI, pursuant to the Memorandum of Agreement between the DNI and the Secretary of Defense, "Management of Acquisition Programs Executed at the Department of Defense Intelligence Community Elements." The DIRNSA/CHCSS shall exercise such delegated MDA, pursuant to delegation instructions and applicable procedures as directed by the Secretary of Defense and the DNI, pursuant to ICD 801 (formerly ICD 105).

(7) Enter into personal-services contracts to the extent permitted by law.

(8) Approve premium-class travel when required for the successful performance of an intelligence mission.

(9) Exercise the authority delegated to the Secretary of Defense by the Administrator of the General Services Administration on the disposal of surplus personal property for responsibilities assigned herein.

(10) Establish and maintain appropriate property accounts for NSA/CSS, appoint Boards of Survey, approve reports of survey, relieve personal liability, and drop accountability for NSA/CSS property contained in the authorized property accounts that has been lost, damaged, stolen, destroyed, or otherwise rendered unserviceable, pursuant to applicable laws and regulations.

g. Training. Establish and administer programs of training as prescribed in DoDI 1430.04 and DoDI 3305.09.

h. Re-Delegation. The DIRNSA/CHCSS may re-delegate these authorities, as appropriate and in writing, except as otherwise restricted in this enclosure or by law or regulation.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ACAT	acquisition category
ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer
CCP	Consolidated Cryptologic Program
CND	computer network defense
CNSS	Committee on National Security Systems
COMSEC	communications security
CSS	Central Security Service
CRITIC	critical information
CRITICOMM	Critical Information Communications
DA&M	Director of Administration and Management
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DDI	Director of Defense Intelligence
DIA	Defense Intelligence Agency
DIOCC	Defense Intelligence Operations Coordination Center
DIRNSA/CHCSS	Director, NSA/Chief, CSS
DoDD	DoD Directive
DoDI	DoD Instruction
DNI	Director of National Intelligence
E.O.	Executive Order
IA	information assurance
IC	Intelligence Community
ICD	Intelligence Community Directive
INFOSEC	information security
ISSP	Information Systems Security Program
JFCC-NW	Joint Functional Component Command for Network Warfare
MDA	Milestone Decision Authority
MIP	Military Intelligence Program
NIP	National Intelligence Program
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
NSS	National Security Systems
OPM	Office of Personnel Management

OPSEC	operations security
PM	Program Manager
SCI	Sensitive Compartmented Information
SCC	Service Cryptologic Component
SIGINT	signals intelligence
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USG	United States Government
USSTRATCOM	United States Strategic Command

PART II. DEFINITIONS

Unless otherwise noted, the following terms and definitions are for the purpose of this Directive:

CCP. That part of the NIP that funds the national-level U.S. SIGINT mission, i.e., collection, processing, retention, and dissemination of information obtained by exploiting foreign communications and non-communications signals on behalf of national-level consumers.

CND. Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks.

COMSEC. Measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

computer network attack. Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

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, or persons, or their agents, or international terrorist organizations or activities.

CRITIC. Critical information messages sent over the CRITICOMM System that must be delivered to the President within 10 minutes upon recognition.

critical information. Decisions, intentions, or actions of foreign governments, organizations, or individuals that could imminently and materially jeopardize vital U.S. policy, economic,

informational, or military interests to such an extent that the immediate attention of the President and the National Security Council may be required.

CRITICOMM System. Communications system developed by NSA to ensure critical information would be delivered to the President within 10 minutes upon recognition. Messages sent on the system are called CRITICs.

cryptography. The art and science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

cryptology. The science that deals with hidden, disguised, or encrypted communications. It includes COMSEC and communications intelligence.

Defense Intelligence. 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 that is significant to Defense policy-making or the planning and conduct of military operations and activities.

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

Functional Manager. Pursuant to E.O. 12333, Functional Managers shall report to the DNI concerning the extent of their duties as Functional Managers, and may be charged with developing and implementing strategic guidance, policies, and procedures for activities related to a specific intelligence discipline or set of intelligence activities; setting training and tradecraft standards; and ensuring coordination within and across intelligence disciplines and IC elements and with related non-intelligence activities. Functional Managers may also advise on resource management; policies and procedures; collection capabilities and gaps; intelligence processing and dissemination; technical architectures; and other issues or activities, as applicable.

IA. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

INFOSEC. Refers to the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

ISSP. Provides financial and manpower resources for efforts directed at protecting information systems from unauthorized access or modification of information, and against the denial of service to authorized users or provision of service to unauthorized users. It addresses the

confidentiality, authenticity, integrity, non-repudiation, and availability of information processed on DoD information systems.

MIP. The program that covers Defense Intelligence requirements, and funds Defense-wide/joint SIGINT activities of NSA/CSS and the SCCs; intelligence, surveillance, and reconnaissance capabilities; and intelligence support to information operations.

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 U.S. department or agency or by the President. It 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 U.S. Armed Forces.

NSS. As provided for in section 3542(b)(2) of title 44, U.S.C., and other applicable law and policy direction, "NSS" means any information system (including any telecommunications system) that is protected at all times by procedures established for information specifically authorized under criteria established by an E.O. or an Act of Congress to be kept classified in the interest of National Defense or foreign policy. However, the term also includes any unclassified information system (including any telecommunications system) used or operated by an agency, an agency contractor, or other organization on behalf of an agency, where the function, operation, or use of that system involves (i) intelligence activities, (ii) cryptologic activities related to national security, (iii) command and control of military forces, (iv) equipment that is an integral part of a weapon or weapon systems, or (v) systems critical to the direct fulfillment of military or intelligence missions; it excludes any system that is designed to be used for routine administrative and business applications such as payroll, finance, logistics, or personnel management applications.

OPSEC. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to identify those actions that can be observed by adversary intelligence systems; determining indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and selecting and executing measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

PM. The designated individual with responsibility for and authority to accomplish program objectives for development, production, and sustainment to meet the user's operational needs.

SCCs. Term used to designate, separately or collectively, elements of the Army, Navy, Marine Corps, Air Force, and Coast Guard assigned to the CSS by the Secretary of Defense for the conduct of cryptologic operations funded by NSA/CSS. The Commanders of the SCCs represent the interests of their Military Service cryptologic force.

SIGINT. The category of intelligence which includes, individually or in combination, all communications, electronic, or foreign instrumentation signals intelligence.