Department of Defense
DIRECTIVE

NUMBER 5143.01
October 24, 2014
Incorporating Change 2, April 6, 2020

CMO

SUBJECT: Under Secretary of Defense for Intelligence and Security (USD(I&S))

References: See Enclosure

1. PURPOSE. This directive:

a. Reissues DoD Directive (DoDD) 5143.01 (Reference (a)) to update the responsibilities and functions, relationships, and authorities of the USD(I&S), pursuant to the authority vested in the Secretary of Defense (SecDef) by sections 113 and 137 of Title 10, United States Code (U.S.C.) (Reference (b)), and in accordance with section 3001 *et seq.* of Title 50, U.S.C. (Reference (c)), as well as Public Law 108-458 (Reference (d)), Executive Order (E.O.) 12333 (Reference (e)), E.O. 13470 (Reference (f)), and E.O. 13869 (Reference (g)).

b. Authorizes the USD(I&S) to reissue chartering DoDDs, in accordance with DoD Instruction (DoDI) 5025.01 (Reference (h)), for OSD Presidentially-appointed, Senate-confirmed officials, who are under the authority, direction, and control of the USD(I&S).

c. Conforms to and is consistent with law and Presidential guidance concerning the authorities and responsibilities of the Director of National Intelligence (DNI).

d. Cancels Deputy Secretary of Defense (DepSecDef) Memorandums (References (i) and (j)).

2. APPLICABILITY. This directive applies to OSD, the Military Departments (MILDEPs), the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands (CCMDs), 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 DoD (referred to collectively in this directive as the "DoD Components").

3. RESPONSIBILITIES AND FUNCTIONS. The USD(I&S) is the Principal Staff Assistant (PSA) and advisor to the SecDef and DepSecDef regarding Intelligence, Counterintelligence (CI), Security, sensitive activities, and other intelligence-related matters (referred to in this directive as "assigned responsibilities" or "Defense Intelligence, CI, and Security"). In this

capacity, the USD(I&S) exercises SecDef authority, direction, and control over, and oversees the activities of, the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Security Agency/Central Security Service (NSA/CSS), the National Reconnaissance Office (NRO), and the Defense Counterintelligence and Security Agency; and exercises planning, policy, and strategic oversight for all associated policy, plans, and programs. In the exercise of assigned responsibilities, the USD(I&S):

a. Serves as the senior Defense Intelligence, CI, and Security official below the SecDef and DepSecDef.

b. Engages the National Security Council (NSC) staff, other government agencies (OGAs), and DoD Components to develop policies, plans, and programs to enable operational application of Defense Intelligence and other capabilities, as appropriate. Provides the NSC principals and deputies committees with Defense Intelligence, CI, Security, sensitive activities, and special program perspectives, in coordination with the Under Secretary of Defense for Policy (USD(P)). Ensures DoD intelligence and intelligence-related sensitive activities and special access programs (SAPs) align with SecDef and U.S. Government (USG) guidance.

c. Serves as Director of Defense Intelligence and principal advisor to the DNI on Defense Intelligence matters, in accordance with the SecDef and DNI Memorandum of Agreement (Reference (k)), and as the primary SecDef representative to the Office of the DNI (ODNI) and all other Intelligence Community (IC) elements regarding the responsibilities and functions prescribed in this directive.

d. Serves as the DoD senior official for the insider threat program; develops policy and guidance and oversees implementation of the DoD insider threat program; and makes resource recommendations to implement requirements, in accordance with E.O. 13587, Presidential Memorandum, and DoDD 5205.16 (References (l), (m), and (n)).

e. Facilitates integration of Defense Intelligence and DoD support with IC activities.

f. Establishes policy and priorities for, and provides oversight of, the Defense Intelligence Enterprise, including pursuant to DoDD 5240.01 (Reference (o)) and other SecDef and DNI guidance. Ensures DoD IC elements are responsive and timely with respect to satisfying the needs of operational military forces, in accordance with section 3038 of Reference (c).

g. For Defense Intelligence:

(1) For Defense Intelligence analysis:

(a) Provides oversight and guidance to ensure the analysis meets DoD policy, operations, planning, and acquisition requirements; supports timely and accurate decision-making; and is available to support national requirements.

(b) Provides oversight and direction for capabilities and the implementation of policies, plans, and programs to ensure effective support to the DoD mission.

(c) Ensures the analysis is aligned with IC and DoD analytical concepts, methodologies, and tradecraft efforts.

(2) For Defense human intelligence (HUMINT):

(a) Establishes policy and provides oversight and direction, in accordance with DoDD S-5200.37 (Reference (p)). Serves as DoD representative to the IC for Defense HUMINT policy and related matters.

(b) Provides oversight and direction to ensure Defense HUMINT Executors are organized and structured to support the missions of DoD and the requirements of the OSD and DoD Components and ODNI, in accordance with Reference (p).

(c) Identifies DoD-related National Intelligence requirements to guide Defense HUMINT activities. Facilitates and guides Defense HUMINT activities and source operations, in consultation with the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, as appropriate, in accordance with Reference (p) and DoDD S-3325.09, Intelligence Community Directive 310, and IC Directive 304 (References (q), (r), and (s)).

(d) Oversees the integration and delivery of actionable HUMINT to the warfighter through clandestine tradecraft, technologies, methodologies, and processes.

(3) For technical collection (i.e., signals intelligence, geospatial intelligence, measurement and signature intelligence, and biometrics-enabled and forensics-enabled intelligence):

(a) Provides oversight and direction of technical collection capabilities, including technical collection support, to the DoD. Ensures NSA/CSS, NGA, DIA, and NRO, in the execution of their missions, fully support the operations, policy, planning, and acquisition requirements of DoD and the USG, as appropriate.

(b) Develops and provides policy and implementation guidance for the synchronization and operational integration across the technical collection disciplines and for the synchronization and alignment of Defense technical collection operations with national collection operations.

(c) Oversees the collection prioritization processes and synchronization between national and Defense collection prioritization processes.

(4) For Defense open source intelligence:

(a) Provides oversight and direction of capabilities, policies, plans, and programs. Ensures activities support DoD missions and satisfy the needs of the MILDEPs and the CCMDs.

(b) Ensures strategies, policies, guidance, and activities are synchronized with those of the IC.

(5) Appoints the Defense Collection Manager and provides oversight and direction of DoD collection management policies, plans, and programs.

h. For Defense CI activities:

(1) Represents the SecDef at the National CI Executive, the National CI Policy Board, and other U.S. and international CI community forums.

(2) Develops and oversees implementation of policy, programs, guidance, and training. Monitors and oversees activities, programs, and resources to ensure compliance with DoD and national CI policies.

(3) Strengthens, oversees, and directs CI policy and program oversight to leverage capabilities and capacity to address validated DoD and national CI priorities.

(4) Develops and oversees DoD credibility assessment policies, and ensures that DoD supports credibility assessment requirements identified by the OGA heads.

i. For all intelligence and intelligence-related sensitive activities, and related matters:

(1) Establishes policy and provides oversight and direction for the coordination, assessment, reporting, and conduct of DoD intelligence and intelligence-related sensitive activities, the Defense Cover Program, special communications, technical collection support to intelligence activities, and the clandestine use of technology.

(2) Establishes policy and provides oversight and direction for the provision of Defense sensitive support to the DoD Components and OGAs, in accordance with DoDD S-5210.36 (Reference (t)).

(3) Provides policy and operations advice to the SecDef and NSC principals on sensitive activities undertaken by OGAs.

(4) Serves as the DoD Functional Manager for Special Communications, in accordance with DoDI S-3200.17 (Reference (u)).

j. For Defense Security Programs and associated matters:

(1) Serves as the DoD Senior Agency Official for Security pursuant to E.O.s 13526, 13556, 13549, and 12977 (References (v), (w), (x), and (y)), and advises the SecDef, Secretaries of the MILDEPs, CJCS, and other DoD Component heads on the development and integration of risk-managed security policies and programs, except for those related to nuclear, chemical, and biological security. Represents the SecDef at national-level security forums.

(2) Establishes policy and an integrated strategic framework for the management and oversight of the Defense Security Enterprise, in accordance with DoDD 5200.43 (Reference (z)).

(3) Develops personnel security policy and guidance, and oversees the DoD

implementation of E.O.s 12968 and 13467 (References (aa) and (ab)), Reference (g), and the DoD Personnel Security Program.

(4) Performs all SecDef duties and responsibilities regarding the physical security program, pursuant to Reference (y). Develops physical security policy and guidance, and oversees DoD implementation of section 797 of Reference (c), section 1382 of Title 18, U.S.C., section 1069 of Public Law 110-181 (References (ac), and (ad)), and the DoD Physical Security Program.

(5) Develops information security policy and guidance and oversees DoD implementation of References (v), (w), and (x), and the DoD Information Security Program.

(6) Performs all SecDef duties and responsibilities regarding the National Industrial Security Program, pursuant to E.O. 12829 (Reference (ae)). Develops industrial security policy and guidance, and oversees DoD implementation of Reference (z) and the DoD Industrial Security Program.

(7) Oversees the implementation of policy regarding the protection of sensitive compartmented information, pursuant to Presidential and DNI guidance.

(8) Develops and oversees implementation of DoD SAP security policy, pursuant to DoDD 5205.07 (Reference (af)).

(9) Provides policy and direction for the identification, reporting, investigation, and referral of serious security incidents, including unauthorized disclosures of classified information.

(10) Develops and oversees implementation of policy and guidance for critical program information identification and protection, in coordination with the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)).

(11) Provides policy and direction for the investigative and adjudicative guidance for issuing the common access card, in accordance with Homeland Security Presidential Directive-12, Federal Information Processing Standards Publication 201-2, and Office of Personnel Management Memorandum (References (ag), (ah), and (ai)).

k. For operational support:

(1) Consults with CJCS for operational support matters.

(2) Develops and oversees implementation of policy, programs, plans, and guidance for Defense Intelligence warfighting support to the CCMDs. Evaluates and oversees DIA, NSA/CSS, NGA, and NRO activities to ensure effective support to DoD and USG interagency operations and activities.

(3) Reviews and advocates for intelligence capabilities of the Joint Intelligence Operations Centers and the Service Intelligence Centers, in coordination with the CCMDs and

MILDEPs, to ensure mission performance is aligned with Defense priorities and consistent with national priorities.

(4) Provides guidance and oversight of the Defense Intelligence Components for intelligence planning and intelligence support to joint targeting for the CCMDs.

(5) Develops and oversees implementation of DoD policy, strategy, programs, and guidance on all intelligence, surveillance, and reconnaissance (ISR) manned and unmanned spaceborne, airborne, surface, subsurface, and cyberspace activities, and associated tasking, processing, exploitation, and dissemination. Provides DoD-wide focus and advocacy for ISR capabilities and integrated tasking, processing, exploitation, and dissemination solutions. Coordinates, oversees, and assesses efforts of the DoD Components and proposes options to optimize integrated ISR capabilities.

(6) Identifies and recommends solutions to resource, program for, and resolve challenges associated with deploying and optimizing ISR capability in response to gaps identified in planning and during the conduct of operations.

(7) Executes and provides oversight of program policy for reconnaissance and surveillance activities and operations. Serves as the DoD principal for interagency coordination on the Sensitive Reconnaissance Operations schedule and requirements. Provides expertise on matters of technical collection and operational employment. Represents the DoD on Sensitive Reconnaissance Operations and ISR-related activities in national and international forums.

(8) Participates in capabilities-development processes (e.g., the Joint Capabilities Integration and Development System) to identify and assess Joint Military Intelligence, CI, and Security capability needs in order to provide capabilities required by the warfighters.

(9) In coordination with the USD(P), develops and oversees implementation of DoD policy, programs, and guidance for the congruent application of military deception and operations security, in accordance with DoDD 5205.02E (Reference (aj)), in support of missions and operations, ensuring shared responsibility and close synchronization with intelligence, operations, and associated planning elements.

l. For international intelligence engagement:

(1) Oversees the development, management, and coordination of intelligence and CI relationships between Defense intelligence and CI elements and foreign governments and international organizations.

(2) Develops mechanisms to advance and synchronize intelligence relationships between Defense intelligence and CI elements and foreign governments and international organizations.

(3) Establishes and maintains Defense Intelligence relationships and Defense Intelligence exchange programs with selected cooperative foreign defense establishments, intelligence or security services of foreign governments, and international organizations, in

coordination with the USD(P). Ensures that such relationships and programs are in accordance with Reference (e) and DoDI 5530.03 (Reference (ak)). Such relationships will be established and maintained in consultation with the Combatant Commanders (CCDRs), as appropriate.

m. For the DoD Foreign Materiel Program (FMP):

(1) Provides strategic guidance on all bi-lateral and multi-lateral engagements. Develops and oversees the DoD FMP through policy, plans, and strategic guidance for the acquisition and technical exploitation of foreign materiel or technology. Provides plans and strategic guidance to the Military Services through the Secretaries of the MILDEPs, and to the Defense Intelligence Component heads. Oversees high risk, high cost, or highly sensitive FMP-related activities.

(2) Establishes, programs, budgets, and executes the OSD foreign materiel acquisition and exploitation fund in support of DoD foreign materiel activities.

n. For intelligence information sharing:

(1) Establishes and oversees the implementation of Defense Intelligence policy, guidance, and strategy for intelligence information sharing, in accordance with applicable laws, regulations, and DoD and IC policy, including References (e), (f), (v), (w); DoDDs 5205.15E, 8521.01E, and 5250.01 (References (al), (am), and (an)); and E.O. 13388 (Reference (ao)) and Reference (l).

(2) Synchronizes and facilitates intelligence information sharing activities across the Defense Intelligence Enterprise with the CCMDs, Joint Staff, ODNI, other IC elements, OGAs, and allied and coalition mission partners.

(3) Provides intelligence information sharing assistance in support of Homeland Defense, as requested, in coordination with the USD(P), the CJCS, and the DoD Component heads.

(4) Makes disclosure and release decisions for Military Intelligence to foreign governments and international organizations, in accordance with National Disclosure Policy-1 (Reference (ap)) and National Intelligence sharing guidance, as appropriate. Oversees implementation of foreign disclosure of Military Intelligence in consultation with the USD(P).

o. For cyberspace capabilities and activities supporting cyberspace operations related to responsibilities assigned in this directive, consistent with section 932 of Public Law 113-66 (Reference (aq)):

(1) Develops and oversees policy, programs, and guidance, with an emphasis on operations support to the MILDEPs and CCMDs, in coordination with the USD(P), other OSD PSAs, and CJCS, as applicable. Accounts for DoD investments in cyberspace capabilities to meet warfighter requirements.

(2) Ensures the development of balanced intelligence support to the cyberspace operations portfolio that is integrated with the activities of the DoD Components and interagency

and allied partners.

(3) Coordinates future research and strategic information environment forecasts to inform DoD and Defense Intelligence policy and investments for long-range planning and implementation of intelligence capabilities and capacity supporting cyberspace operations. Leverages DoD research and development with commercial, academic, and other relationships, in coordination with the Under Secretary of Defense for Research and Engineering (USD(R&E)), to rapidly develop and institutionalize new technology, concepts, and capabilities.

p. For Defense Intelligence Enterprise mission support:

(1) Develops and implements strategy, strategic plans, and other strategic guidance, in consultation with the DoD Component heads and the DNI, as appropriate.

(2) Regarding planning, programming, budgeting, and execution (PPBE) and other budgetary matters:

(a) Coordinates with the DNI on strategy development, PPBE, and evaluation of national IC programs and jointly funded programs.

(b) Participates in the DoD PPBE process, in accordance with section 135 of Reference (b), provides perspectives and forecasts on threats and the impact of resource decisions, identifies priorities, proposes programmatic and fiscal guidance, and develops budget justification material.

(c) As the Military Intelligence Program (MIP) Executive, pursuant to DoDD 5205.12 (Reference (ar)) and Reference (k), provides policy guidance and oversight to the Defense Intelligence, CI, and Security plans, programs, required capabilities, and resource allocations by exercising responsibility with respect to the DoD Components within the MIP and the National Intelligence Program (NIP). Coordinates with ODNI to develop, synchronize, and implement annual NIP and MIP priorities.

(d) Oversees all Defense Intelligence, CI, and Security budgetary matters. Consults and coordinates with the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense (USD(C)/CFO), on MIP budgetary matters, and the DNI on MIP and NIP budgetary matters. Consults and coordinates with the MILDEPs on intelligence and non-intelligence funding associated with Battlespace Awareness Capability Portfolio, in accordance with DoDD 7045.20 (Reference (as)), and security activities.

(e) Manages the Battlespace Awareness Capability Portfolio, pursuant to Reference (as), and oversees planning, organizing, coordinating, and balancing of investment and risk for all DoD ISR and Environmental System Capabilities, and consults with the Commander, U.S. Strategic Command, as appropriate.

(f) Consults and coordinates with the USD(A&S), the USD(R&E), the USD(P), the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), the USD(C)/CFO, the Director of Cost Assessment and Program Evaluation, the Secretaries of the MILDEPs, the

CJCS, and Commander, U.S. Special Operations Command on Defense Intelligence PPBE.

(g) Supports the Assistant Secretary of Defense for Legislative Affairs and USD(C)/CFO in presenting, justifying, and defending Intelligence, CI, and Security programs and budgets before Congress and evaluating and assessing Congressional activity for impact on these issues.

(3) Regarding acquisition and capability matters:

(a) Advises and assists the USD(A&S), DoD Chief Information Officer, Director of Cost Assessment and Program Evaluation, CJCS, and Defense Acquisition Board, as well as the DNI and the OGA heads, as appropriate, concerning acquisition programs that affect Intelligence, CI, and Security capabilities and programs.

(b) Exercises acquisition authority, as delegated by the USD(A&S), DNI, or other appropriate official, for Intelligence, CI, and Security technologies, systems, and equipment.

(c) Ensures the exercise of acquisition authority by the heads of the Defense Intelligence, CI, and Defense Security Components is in coordination with the USD(A&S).

(d) Oversees the development and execution of Military Intelligence and National Intelligence capabilities, in coordination with CJCS and DNI, to support the CCDRs, Defense policy, and the planning and conduct of military operations.

(e) Prioritizes and facilitates the review and fielding of high priority SecDef intelligence programs and intelligence-related quick-reaction capabilities. Identifies and seeks waivers for acquisition-related processes that could delay fielding of intelligence capabilities.

(4) Regarding technology insertion:

(a) Identifies capability gaps and opportunities to enhance Intelligence, CI, and Security capabilities.

(b) Oversees research, development, test, and evaluation, in conjunction with the USD(R&E), the Director of Operational Test and Evaluation, and the DoD Component heads, as appropriate, and in accordance with DoD acquisition regulations and sections 139 and 2399 of Reference (b). NIP-funded programs must be undertaken in coordination with the DNI.

(5) Regarding Defense Intelligence, and designated SAP management and oversight:

(a) Implements guidance provided by the DoD SAP Oversight Committee. Serves as oversight authority for all designated SAPs.

(b) Ensures SAP oversight by establishing a SAP Central Office in the Office of the USD(I&S) and designating a SAP Central Office Director to be responsible for executing the responsibilities outlined in Reference (af):

1. Exercises cognizance and oversight of designated DoD SAPs and personnel granted access to these programs.

2. Manages and oversees DoD Alternative Compensatory Control Measures, consistent with Volume 3 of DoD Manual (DoDM) 5200.01 (Reference (at)).

3. Ensures all NIP-funded DoD SAPs are regularly reviewed for consistency with DNI policy.

(c) Oversees intelligence support to non-USD(I&S) SAPs.

(6) Regarding human capital and manpower management:

(a) Exercises oversight of personnel policy regarding Defense intelligence positions, in accordance with DoDD 1400.35 (Reference (au)), to ensure that the Defense Intelligence Components are staffed, equipped, trained, structured, and ready to support DoD missions and to satisfy the needs of the DoD and the IC, as appropriate.

(b) Develops and oversees implementation of the policies associated with Defense Intelligence positions authorized by Reference (b) in the Defense Civilian Intelligence Personnel System (DCIPS), including Defense Intelligence Senior Executive Service and Defense Intelligence Senior Level positions in conjunction with the USD(P&R), in accordance with Reference (at).

(c) For Defense Intelligence positions, serves in the role assigned to the Director of the Office of Personnel Management for positions and employees under Title 5, U.S.C. (Reference (av)), unless otherwise stated in law or DoD policy.

(d) Develops policy and provides oversight of training (including joint intelligence training), certification, education, and professional development of personnel in Defense Intelligence, CI, and Security Components and ensures integration of Defense intelligence standards into other training within the DoD and IC, as appropriate.

(e) Oversees implementation of DoD detailee policy, within assigned areas of responsibility, for all military and DCIPS personnel. Approval for detailees to external organizations will be in accordance with DoDI 1000.17 and DoDI 1400.36 (References (aw) and (ax)), and Reference (t).

(f) Appoints a senior official to represent Defense Intelligence Enterprise foreign language and foreign area interests, and oversees DoD policy and programs that build, maintain, and employ foreign language and foreign area expertise within the Defense Intelligence Enterprise, pursuant to DoDD 5160.41E (Reference (ay)).

(g) Provides duty performance inputs to the Secretaries of the MILDEPs and solicits evaluative inputs from the DNI, as appropriate, on the intelligence element heads of the MILDEPs.

(h) Coordinates, executes, and oversees the Joint Intelligence Manpower Validation process for the MIP.

(i) Establishes and provides policy guidance, resource advocacy, and oversight for the integration of Reserve Component intelligence elements, and ensures that practices and procedures effectively employ and resource Reserve Component intelligence elements, in accordance with DoDD 1200.17 (Reference (az)).

(7) Serves as DoD focal point for intelligence information systems interoperability and governance processes, in accordance with DoDI 8330.01 (Reference (ba)) and References (l) and (ao). Coordinates, oversees, and assesses efforts of the DoD Components to plan, program, and develop capabilities in support of intelligence information sharing, architectures, and interoperability requirements.

q. Sends reports to the DoD Senior Intelligence Oversight Official (DoD SIOO) within the Office of the Chief Management Officer of the Department of Defense (CMO) or directs DoD Component reporting to the CMO or DoD SIOO when made aware of questionable intelligence activities and significant or highly sensitive matters occurring in Defense Intelligence Components, in accordance with DoD 5240.1-R and DoDD 5148.13 (References (bb) and (bc)).

r. Ensures that policies and programs are designed and managed to improve performance, economy, and efficiency, and that all of the Defense Agencies over which the USD(I&S) exercises SecDef authority, direction, and control are attentive and responsive to their organizational customer requirements, both inside and outside DoD.

s. Develops, implements, and oversees policy, programs, and guidance for mission assurance, in coordination with other DoD Component heads and the DNI.

t. Develops and implements procedures for fulfilling USD(I&S)'s intelligence oversight approval roles, as outlined in References (ba) and DoDM 5240.01 (Reference (bd)).

u. Serves on boards, committees, and other groups pertaining to assigned responsibilities and represents the SecDef on all assigned responsibilities in other USG forums.

v. Periodically assesses any DoD Executive Agent assigments under USD(I&S) cognizance for continued need, currency, effectiveness, and efficiency in satisfying end user requirements, consistent with DoDD 5101.1 (Reference (be)).

w. Performs such other duties as the SecDef or DepSecDef may prescribe.

4. RELATIONSHIPS

a. In the performance of assigned responsibilities, the USD(I&S) is the senior intelligence official in the DoD subject to the authority, direction and control of the SecDef and DepSecDef, and:

(1) Reports directly to the SecDef.

(2) Exercises SecDef authority, direction, and control over the following DoD Component heads:

(a) Director, DIA.

(b) Director, NGA.

(c) Director, NRO.

(d) Director, NSA/Chief, CSS.

(e) Director, DCSA.

(f) Such other positions or organizations as the USD(I&S) may establish, consistent with applicable law, within resources provided by the SecDef. Such authority includes proposing candidates for these positions to the SecDef, pursuant to Reference (e), and is exercised in consultation with the DNI regarding National Intelligence and related matters under DNI's purview, as appropriate.

(3) Serves as SecDef focal point with the NSC staff, the OGAs, and, pursuant to responsibilities and functions prescribed in this directive, Congress, State agencies, foreign governments, and international, commercial, and academic organizations.

(4) Provides recommendations to the USD(C)/CFO on all transfers, realignments, and reprogramming of funds to and from the MIP. Consults with the ODNI in advance of transferring or reprogramming MIP funds. Coordinates or consults with DoD Component heads, as appropriate, on all reprogramming plans. Coordinates with the DNI to ensure effective, complementary, and mutual support between Defense Intelligence programs and the NIP.

(5) Coordinates, as appropriate and as required, with DoD Component heads, OSD PSAs, the Principal Cyber Advisor, the OGA heads, including IC elements, and the DNI regarding all responsibilities and functions in this directive.

(6) Uses existing DoD and OGA systems, facilities, and services, when possible, to avoid duplication and to achieve maximum readiness, sustainability, economy, and efficiency.

(7) Implements DCIPS policy in conjunction with the USD(P&R), pursuant to Reference (a), and provides recommendations to the USD(P&R) regarding supporting data systems, as appropriate.

b. The other OSD PSAs and the DoD Component heads will coordinate with the USD(I&S) on all matters under their purview related to the authorities, responsibilities, and functions assigned in this directive.

c. The CJCS consults with, and seeks the advice of, the CCDRs on policy, programs, and

other related activities that support Defense Intelligence, CI, and Security goals and missions, including requests for advice, resources, assistance, and other functions, in accordance with section 153 of Reference (b). The CJCS facilitates communications with the CCDRs to ensure Defense Intelligence, CI, and Security interoperability and support for joint warfighting, particularly as they relate to intelligence-related functions prescribed in this directive and consistent with sections 164, 167, and 167a of Reference (b).

d. The Defense Intelligence Component heads provide the USD(I&S) with copies of the intelligence estimates or other substantive and time-sensitive intelligence provided to the SecDef, DepSecDef, CJCS, DNI, or other senior officials outside of DoD.

e. The DoD Chief Information Officer, pursuant to DoDD 5144.02 (Reference (bf)), coordinates with the USD(I&S) regarding the NSA/CSS cybersecurity mission and associated budget.

f. The Office of the Inspector General of the Department of Defense and the other Inspectors General within the Department conduct audits, investigations, assessments, and evaluations of projects, programs, and other activities performed by the USD(I&S), in accordance with this directive, and pursuant to the Inspector General Act of 1978 (Reference (bg)) and other applicable DoDDs and DoDIs, including DoDD 5106.01 and DoDI 7050.03 (References (bh) and (bi)).

5. AUTHORITIES. Pursuant to the authority vested in the SecDef, and subject to SecDef authority, direction, and control, and in accordance with DoD policies and issuances, the USD(I&S) is hereby delegated authority to:

a. Exercise, within assigned responsibilities and functional areas, all authority of the SecDef derived from statute, E.O., regulation, or interagency agreement, except where specifically limited by statute or E.O. to the SecDef.

b. Establish DoD policy through DoDIs, directive-type memorandums (DTMs), and rules published in the Federal Register, within the authorities and responsibilities assigned in this issuance and in accordance with Reference (h) or Administrative Instruction 102 (Reference (bj)).

(1) In those documents, assign responsibilities related to the authorities and responsibilities in this issuance to other OSD PSAs and the DoD Component heads. Assignment of responsibilities in DoD issuances or rules published in the Federal Register to Military Department officials must be made through the Secretaries of those Departments. DoD issuances or rules published in the Federal Register assigning responsibilities to the CCMDs must be coordinated with the CJCS.

(2) DoDIs and DTMs must be fully coordinated in accordance with Reference (h). Rules published in the Federal Register must be fully coordinated with impacted OSD and DoD Component heads and be consistent with Reference (bi).

(3) This authority may not be redelegated.

c. Approve other DoDIs, DoDMs, and DTMs in areas of assigned responsibilities and functions that implement policy already established by a DoD directive, DoDI, DTM, or policy memorandum issued by the SecDef or DepSecDef.

(1) In these documents, assign responsibilities related to the authorities and responsibilities in this issuance to other OSD PSAs and the DoD Component heads. Assignment of responsibilities in these DoD issuances to Military Department officials must be made through the Secretaries of those Departments. DoD Issuances assigning responsibilities to the CCMDs must be coordinated with the CJCS.

(2) Such documents must be fully coordinated in accordance with Reference (h).

(3) This authority may only be further delegated to officials as specified in Reference (h).

d. Approve Federal Register publication of significant guidance documents as defined in E.O. 13891 (Reference (bk)) and determined by the Office of Management and Budget. This authority may not be redelegated.

e. Approve the Federal Register publication of documents other than rules and significant guidance documents (e.g., notices, orders, and non-significant guidance documents as defined by Reference (bk) and determined by the Office of Management and Budget) in accordance with Reference (bi). Unless otherwise restricted by law, this authority may be further delegated only in writing to officials at or above the level of a general or flag officer, Senior Executive Service member, or equivalent.

f. Reissue, when necessary, in accordance with Reference (h), chartering DoDDs for those OSD officials who were appointed by the President with the advice and consent of the Senate and who are under the authority, direction, and control of the USD(I&S). This authority may not be re-delegated. The CMO continues to develop and maintain these chartering DoDDs, in accordance with Reference (h).

g. Obtain reports and information, in accordance with DoDI 8910.01 (Reference (bl)), as necessary, in carrying out assigned responsibilities and functions.

h. Communicate directly with the DoD Component heads, as necessary, to carry out assigned responsibilities and functions, including transmitting requests for advice and assistance. Communications to the MILDEPs must be transmitted through the Secretaries of the MILDEPs, or as otherwise provided in law or directed by the SecDef. Communications to the CCDRs must be in accordance with DoDD 5100.01 (Reference (bm)).

i. Establish arrangements for DoD participation in USG programs for which the USD(I&S) is assigned primary DoD cognizance.

j. Communicate directly with ODNI on Defense Intelligence, CI, and Security matters on behalf of the SecDef.

k. Communicate with OGA officials, members of the public, and representatives of foreign governments and international organizations, and non-governmental organizations, as well as State, local, and tribal entity heads, as appropriate, in carrying out assigned responsibilities and functions. Communications with representatives of the Legislative Branch will be conducted through the Office of the Assistant Secretary of Defense for Legislative Affairs, except for communicating with the Defense Appropriations Committees, which will be coordinated with the Office of the USD(C)/CFO. Communications with representatives of the news media will be conducted through the Office of the Assistant to the Secretary of Defense for Public Affairs, in accordance with DoDD 5122.05 (Reference (bn)).

l. Designate, on behalf of the SecDef, DoD organizational elements that perform intelligence functions as Defense Intelligence Components, with the concurrence of the DoD Component head affected, in accordance with section 1614 of Reference (b). In addition, the DepSecDef, as the head of OSD, delegates to the USD(I&S) authority to concur in such designations for those elements and positions under the USD(I&S).

m. Exercise Top Secret original classification authority and issue appropriate classification guidance, in accordance with Reference (v) and Volume 1 of DoDM 5200.01 (Reference (bo)).

n. Carry out delegations regarding the DCIPS, in accordance with Reference (au).

o. Make determinations relating to personal services contracts that directly support Defense Intelligence, CI, and Security activities, in accordance with section 129b(d)(1)(B) of Reference (b).

p. Waive prohibitions of award of certain contracts to entities controlled by a foreign government, on behalf of the SecDef, pursuant to section 2536(b) of Reference (b).

q. Exercise the authority granted to the SecDef under section 2682 of Reference (b) to waive the requirements of subsections (a) and (b) of that section.

r. In coordination with the USD(A&S), exercise the authority granted to the SecDef under section 3304 of Reference (c) to make a joint determination with the DNI and submit the required report.

s. Negotiate and conclude agreements with DoD Components, OGAs, and State or local governments as necessary to carry out assigned responsibilities.

t. Enter into support agreements, as required, for the effective performance of responsibilities and functions assigned to the USD(I&S), in accordance with DoDI 4000.19 (Reference (bp)) and the February 13, 2020 DepSecDef Memorandum (Reference (bq)).

u. In consultation with the DNI and the Director of the Federal Bureau of Investigation, as appropriate, make determinations, except for those related to nuclear, chemical, and biological security, on behalf of the SecDef and notify Congress, as required by section 2723 of Reference (b).

v. Exercise the authorities and carry out the responsibilities of the SecDef specified in sections 431 through 437 of Reference (b), except for approval of intelligence commercial activities, which must be accomplished by the SecDef or DepSecDef.

6. RELEASABILITY. **Cleared for public release**. This directive is on the Directives Division Website at https://www.esd.whs.mil/DD/.

7. SUMMARY OF CHANGE 2. The changes to this issuance are administrative and:

a. Update the organizational title of the Under Secretary of Defense for Intelligence to the USD(I&S), pursuant to Section 1621 of the National Defense Authorization Act for Fiscal Year 2020, Public Law 116-92 (Reference (br)).

b. Update the organizational title of the Defense Counterintelligence and Security Agency, as required by Reference (g) and implemented by the June 20, 2019 Acting SecDef Memorandum (Reference (bs)).

c. Update references and organizational symbols to reflect the reorganization of the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, in accordance with the July 13, 2018 DepSecDef Memorandum (Reference (bt)) and the CMO, in accordance with the February 1, 2018 SecDef Memorandum (Reference (bu)).

d. Remove the relationship between USD(I&S) and the Principal DoD Space Advisor involvement in space matters, pursuant to Section 1601 of the National Defense Authorization Act for Fiscal Year 2018, Public Law 115-91 (Reference (bv)).

e. Update the USD(I&S) responsibilities and functions, relationships, and authorities for consistency with those common across OSD PSAs, in coordination with the Office of the General Counsel of the Department of Defense.

8. EFFECTIVE DATE. This directive is effective October 24, 2014.

Chuck Hagel
Secretary of Defense

Enclosure
References
Glossary

ENCLOSURE

REFERENCES

(a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005 (hereby cancelled)
(b) Title 10, United States Code
(c) Title 50, United States Code
(d) Public Law 108-458, "Intelligence Reform and Terrorism Prevention Act of 2004," December 17, 2004
(e) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(f) Executive Order 13470, "Further Amendments to Executive Order 12333, United States Intelligence Activities," July 30, 2008
(g) Executive Order 13869, "Transferring Responsibility for Background Investigations to the Department of Defense," April 24, 2019
(h) DoD Instruction 5025.01, "DoD Issuances Program," August 1, 2016, as amended
(i) Deputy Secretary of Defense Memorandum, "Transfer of Under Secretary of Defense for Intelligence Principal Staff Assistant Responsibilities for DoD Chemical and Biological Security Policy," June 3, 2012 (hereby cancelled)
(j) Deputy Secretary of Defense Memorandum, "Designation of the Department of Defense Senior Agency Official for State, Local, Tribal, and Private Sector Entities Program," October 15, 2012 (hereby cancelled)
(k) Memorandum of Agreement between Secretary of Defense and Director of National Intelligence, "Director of Defense Intelligence," May 21, 2007
(l) Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011
(m) Presidential Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," November 21, 2012
(n) DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014, as amended
(o) DoD Directive 5240.01, "DoD Intelligence Activities," August 27, 2007, as amended
(p) DoD Directive S-5200.37, "Management and Execution of Defense Human Intelligence (HUMINT) (U)," February 9, 2009, as amended
(q) DoD Directive S-3325.09 "Oversight Management, and Execution of Defense Clandestine Source Operation (U)," January 9, 2013, as amended
(r) Intelligence Community Directive 310, "Coordination of Clandestine Human Source and Human-Enabled Foreign Intelligence Collection and Counterintelligence Activities Outside the United States," June 27, 2016
(s) Intelligence Community Directive 304, "Human Intelligence," March 6, 2008, as amended
(t) DoD Directive S-5210.36, "Provision of DoD Sensitive Support to DoD Components and other Departments and Agencies of the U.S. Government (U)," November 6, 2008, as amended
(u) DoD Instruction S-3200.17, "Implementing Instructions for the DoD Special Communications Enterprise Office (SCEO) (U)," July 15, 2009

(v) Executive Order 13526, "Classified National Security Information," December 29, 2009, as amended
(w) Executive Order 13556, "Controlled Unclassified Information," November 4, 2010
(x) Executive Order 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," August 18, 2010
(y) Executive Order 12977, "Interagency Security Committee," October 19, 1995
(z) DoD Directive 5200.43, "Management of the Defense Security Enterprise," October 1, 2012, as amended
(aa) Executive Order 12968, "Access to Classified Information," August 2, 1995, as amended
(ab) Executive Order 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," June 30, 2008, as amended
(ac) Title 18, United States Code
(ad) Public Law 110-181, "National Defense Authorization Act for Fiscal Year 2008," January 28, 2008
(ae) Executive Order 12829, "National Industrial Security Program," January 6, 1993, as amended
(af) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010, as amended
(ag) Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
(ah) Federal Information Processing Standards Publication 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors," August 2013
(ai) Office of Personnel Management Memorandum, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12," July 31, 2008
(aj) DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012, as amended
(ak) DoD Instruction 5530.03, "International Agreements," December 4, 2019
(al) DoD Directive 5205.15E, "DoD Forensic Enterprise (DFE)," April 26, 2011, as amended
(am) DoD Directive 8521.01E, "Department of Defense Biometrics," January 13, 2016, as amended
(an) DoD Directive 5250.01, "Management of Intelligence Mission Data (IMD) in DoD Acquisition," January 22, 2013, as amended
(ao) Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," October 25, 2005
(ap) National Disclosure Policy-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," (short title: National Disclosure Policy (NDP-1)), February 14, 2017[1]
(aq) Public Law 113-66, "National Defense Authorization Act for Fiscal Year 2014," December 26, 2013
(ar) DoD Directive 5205.12, "Military Intelligence Program (MIP)," November 14, 2008, as amended
(as) DoD Directive 7045.20, "Capability Portfolio Management," September 25, 2008, as amended
(at) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection Of Classified Information," February 24, 2012, as amended

[1] Release controlled by the Executive Secretariat of the National Disclosure Policy Committee, (571) 372-2479

(au) DoD Directive 1400.35, "Defense Civilian Intelligence Personnel System (DCIPS)," September 24, 2007, as amended
(av) Title 5, United States Code
(aw) DoD Instruction 1000.17, "Detail of DoD Personnel to Duty Outside the Department of Defense," October 30, 2013
(ax) DoD Instruction 1400.36, "DoD Implementation of the Joint Intelligence Community Duty Assignment (JDA) Program," June 2, 2008
(ay) DoD Directive 5160.41E, "Defense Language, Regional Expertise, and Culture (LREC) Program," August 21, 2015, as amended
(az) DoD Directive 1200.17, "Managing the Reserve Components as an Operational Force," October 29, 2008
(ba) DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," May 21, 2014, as amended
(bb) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 7, 1982, as amended
(bc) DoD Directive 5148.13, "Intelligence Oversight," April 26, 2017
(bd) DoD Manual 5240.01, "Procedures Governing The Conduct Of DoD Intelligence Activities," August 8, 2016
(be) DoD Directive 5101.01, "DoD Executive Agent," September 3, 2002, as amended
(bf) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended
(bg) Inspector General Act of 1978, as amended, Title 5, United States Code, Appendix
(bh) DoD Directive 5106.01, "Inspector General of the Department of Defense (IG DoD)," April 20, 2012, as amended
(bi) DoD Instruction 7050.03, "Office of the Inspector General of the Department of Defense Access to Records and Information," March 22, 2013
(bj) Administrative Instruction 102, "Office of the Secretary of Defense (OSD) Federal Register (FR) System," November 6, 2006, as amended
(bk) Executive Order 13891, "Promoting the Rule of Law Through Improved Agency Guidance Documents," October 9, 2019
(bl) DoD Instruction 8910.01, "Information Collecting and Reporting," May 19, 2014
(bm) DoD Directive 5100.01, "Functions of the Department of Defense and Its Major Components," December 21, 2010
(bn) DoD Directive 5122.05, "Assistant to the Secretary of Defense for Public Affairs (ATSD(PA))," August 7, 2017
(bo) DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, as amended
(bp) DoD Instruction 4000.19, "Support Agreements," April 25, 2013, as amended
(bq) Deputy Secretary of Defense Memorandum, "Delegation of Authority for OSD Component Heads to Enter into Support Agreements," February 13, 2020
(br) Public Law 116-92, "National Defense Authorization Act for Fiscal Year 2020," December 20, 2019
(bs) Acting Secretary of Defense Memorandum, Renaming the Defense Security Service as the Defense Counterintelligence and Security Agency," June 20, 2019
(bt) Deputy Secretary of Defense Memorandum, "Establishment of the Office of the Under Secretary of Defense for Research and Engineering and the Office of the Under Secretary of Defense for Acquisition and Sustainment," July 13, 2018

(bu) Secretary of Defense Memorandum, "Disestablishment of the Deputy Chief Management Officer and Establishment of the Chief Management Officer," February 1, 2018
(bv) Public Law 115-91, "National Defense Authorization Act for Fiscal Year 2018," December 12, 2017
(bw) Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CCDR	Combatant Commander
CCMD	Combatant Command
CI	counterintelligence
CJCS	Chairman of the Joint Chiefs of Staff
CMO	Chief Management Officer of the Department of Defense
DCIPS	Defense Civilian Intelligence Personnel System
DepSecDef	Deputy Secretary of Defense
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
DTM	directive-type memorandum
E.O.	Executive order
FMP	Foreign Materiel Program
HUMINT	human intelligence
IC	Intelligence Community
ISR	intelligence, surveillance, and reconnaissance
MILDEPs	Military Departments
MIP	Military Intelligence Program
NGA	National Geospatial-Intelligence Agency
NIP	National Intelligence Program
NRO	National Reconnaissance Office
NSA/CSS	National Security Agency/Central Security Service
NSC	National Security Council
ODNI	Office of the Director of National Intelligence
OGA	other government agency
PPBE	Planning, Programming, Budgeting, and Execution
PSA	Principal Staff Assistant
SAP	Special Access Program
SecDef	Secretary of Defense

U.S.C.	United States Code
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USD(R&E)	Under Secretary of Defense for Research and Engineering
USG	United States Government

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this directive:

CI. Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons or their agents, or international terrorist organizations or activities.

Defense Intelligence. The integrated Departmental intelligence that covers the broad aspects of national policy and national security and relates 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 USG policy-making or the planning and conduct of military operations and activities. It includes military, strategic, operational, and tactical intelligence.

Defense Intelligence Components. All DoD organizations that perform National Intelligence, Defense Intelligence, and intelligence-related functions, including: the DIA, the NGA, the NRO, the NSA/CSS, and the intelligence elements of the Active and Reserve Components of the MILDEPs, including the United States Coast Guard when operating as a service in the Department of the Navy. The offices and staffs of the senior intelligence officers of the CCMD Headquarters are designated as Defense Intelligence Components, in accordance with Reference (bc).

Defense Intelligence Enterprise. The organizations, infrastructure, and measures to include policies, processes, procedures, and products of the Intelligence, CI, and Security Components of the Joint Staff, CCMDs, MILDEPs, and other DoD elements that perform National Intelligence, Defense Intelligence, intelligence-related, CI, and security functions, as well as those organizations under the authority, direction, and control of the USD(I&S).

Defense Security Components. All DoD organizations that perform security functions, including the-Defense Counterintelligence and Security Agency and the security elements of the MILDEPs, including the United States Coast Guard when operating as part of the Department of the Navy.

Defense Security Enterprise. The organizations, infrastructure, and measures (including policies, processes, procedures, and products) in place to safeguard DoD personnel, information, operations, resources, technologies, and facilities against harm, loss, or hostile acts and influences. This system of systems comprises personnel, physical, industrial, information, operations, as well as SAP security policy, critical program information and protection policy, and security training. It addresses, as part of information security, classified information, including sensitive compartmented information, and controlled unclassified information. It aligns with CI, information assurance, foreign disclosure, security cooperation, technology transfer, export control, cyber security, nuclear physical security, chemical and biological security, antiterrorism, force protection, and mission assurance policy and is informed by other security-related efforts.

HUMINT Executors. The senior DoD intelligence officials, as designated by the DoD Component heads, who are authorized to conduct HUMINT and related intelligence activities, e.g., DIA Deputy Director of HUMINT and the senior intelligence official, as designated by the Secretaries of the MILDEPs for the Army, Navy, Air Force, and Marine Corps, and by the CCDRs.

insider threat. Defined in Reference (m).

ISR. Defined in DoD Dictionary of Military and Associated Terms (Reference (bw)).

Military Intelligence. Collection, analysis, production, and dissemination of information relating to any foreign military or military-related situation or activity that is significant to military policy-making or the planning and conduct of military operations and activities.

National Intelligence. Defined in Reference (e).

sensitive activities. Operations, actions, activities, or programs that, if compromised, could have enduring adverse effects on U.S. foreign policy, DoD activities, or military operations, or cause significant embarrassment to the U.S., its allies, or the DoD. These are generally handled through special access, compartmented, or other sensitive control mechanisms.

sensitive compartmented information. Defined in Reference (bw).