



Department of Defense

DIRECTIVE

NUMBER 5200.43

October 1, 2012

USD(I)

SUBJECT: Management of the Defense Security Enterprise

References: See Enclosure 1

1. PURPOSE. Pursuant to the authorities in paragraph 1.10(h) of Executive Order 12333 (Reference (a)) and consistent with the delegations of authority in DoD Directive (DoDD) 5143.01 (Reference (b)), this Directive:

a. Establishes policy and assigns responsibilities for the management of the Defense Security Enterprise (DSE).

b. Establishes the DSE Executive Committee (DSE ExCom) and provides direction for a comprehensive DSE policy and oversight framework and governance structure to safeguard personnel, information, operations, resources, technologies, and facilities against harm, loss, or hostile acts and influences.

c. Deconflicts the DSE from other DoD security related functions such as force protection and provides for the alignment, synchronization, support, and integration of those related security functions.

d. Assigns responsibilities related to the DSE to the Defense Security Executive.

e. Provides a common lexicon for the DSE.

2. APPLICABILITY. This Directive:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

b. Shall not alter or supersede the existing authority and policies of the Director of National Intelligence (DNI) regarding the protection of intelligence sources, methods, and activities pursuant to Reference (a) or the authorities delegated by the DNI to the heads of the Intelligence Community elements.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. Security is a mission critical function of the DoD and its proper execution has a direct impact on all DoD missions and capabilities and on the national defense. Therefore:

(1) A DSE ExCom shall provide governance for the strategic administration and policy coordination of the DSE. The DSE ExCom's functions and membership are described in Enclosure 2 of this Directive.

(2) A Defense security framework and strategic plan shall provide an integrated, risk-managed structure to guide DSE policy implementation and investment decisions, and to provide a sound basis for oversight and evolution.

(3) Standardized security processes shall be implemented, to the maximum extent possible and with appropriate provisions for unique missions and security environments, across the enterprise to ensure maximum interoperability, consistent quality assurance, and cost savings.

(4) A core of highly qualified security professionals, certified in accordance with DoD Manual 3305.13 (Reference (c)), who can effectively implement security policy and procedures and anticipate and recommend changes needed to address changing operational requirements, shall manage execution of DSE policy.

(5) DSE investments shall be guided by a capital planning and investment control process that is risk-managed and results-based and that informs the DoD's planning, programming, budgeting, and execution processes.

b. The DSE shall measure performance in relation to DoD mission impact.

(1) Security risk management practices shall focus on the potential for and degree of risk of loss in relation to the cost or process burden accrued.

(2) Performance measurement requires recognition that the absence of an unwanted event may be evidence of a positive mission impact.

c. The DoD will consider all means in preventing harm of its resources, to include intelligence, information assurance, security, force protection, and mission assurance functions.

d. Security is the personal responsibility of all DoD personnel (military, civilian, and contractor) and its proper implementation will be directed by commanders and other leaders at each level of the DoD and fostered through awareness, education and training, and leadership.

5. RESPONSIBILITIES. See Enclosure 3. See Enclosure 4 for duties of the Defense Security Executive.

6. RELEASABILITY. UNLIMITED. This Directive is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

7. EFFECTIVE DATE. This Directive:

a. Is effective October 1, 2012.

b. Must be reissued, cancelled, or certified current within 5 years of its publication in accordance with DoD Instruction 5025.01 (Reference (d)). If not it will expire effective October 1, 2022 and be removed from the DoD Issuances Website.



Ashton B. Carter
Deputy Secretary of Defense

Enclosures

1. References
2. DSE ExCom
3. Responsibilities
4. Defense Security Executive

Glossary

ENCLOSURE 1

REFERENCES

- (a) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
- (b) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),
November 23, 2005
- (c) DoD Manual 3305.13, "DoD Security Accreditation and Certification," March 14, 2011
- (d) DoD Instruction 5025.01, "DoD Directives Program," September 26, 2012
- (e) DoD Directive 5105.42, "Defense Security Service (DSS)," August 3, 2010
- (f) DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and
Logistics (USD(AT&L)),
December 9, 2005
- (g) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010
- (h) DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P)),
December 8,
1999
- (i) DoD Directive 5124.02, "Under Secretary of Defense for Personnel and Readiness
(USD(P&R)),
June 23, 2008
- (j) DoD Directive 5118.03, "Under Secretary of Defense (Comptroller)/Chief Financial
Officer, Department of Defense (USD(C)/CFO),
April 20, 2012
- (k) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information
Integration/ DoD Chief Information Officer (ASD(NII)/DoD CIO),
May 2, 2005
- (l) DoD Directive 5145.01, "General Counsel of the Department of Defense," May 2, 2001
- (m) DoD Directive 5105.53, "Director of Administration and Management (DA&M),
February 26, 2008
- (n) DoD Instruction 3305.13, "DoD Security Training," December 18, 2007
- (o) DoD Directive 5106.01, "Inspector General of the Department of Defense (IG DoD),
April 20, 2012
- (p) Executive Order 13434, "National Security Professional Development," May 17, 2007
- (q) Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms," current edition
- (r) Section 401a(4) of title 50, United States Code
- (s) DoD Directive 8500.01E, "Information Assurance (IA),
October 24, 2002

ENCLOSURE 2

DSE EXCOM

1. PURPOSE. The DSE ExCom shall be the senior-level governance body for the strategic administration and policy coordination of the DSE. In that role, it shall:

a. In accordance with Reference (b), advise the Under Secretary of Defense for Intelligence (USD(I)), as the Defense Senior Security Official, on security policy and training; provide recommendations on key policy decisions and opportunities for standardization and improved effectiveness and efficiency; and facilitate cross-functional security policy coordination.

b. Assist with development of a Defense security framework that integrates, across all security levels, personnel, physical, industrial, information, operations, and chemical and biological security, as well as special access program (SAP) security policy, critical program information protection policy, and security training. This framework must align with and be informed by other DoD security and security-related functions (e.g., counterintelligence, information assurance, nuclear physical security, foreign disclosure, security cooperation, technology transfer, export control, cyber security, anti-terrorism, force protection, mission assurance, critical infrastructure, and insider threat policy).

c. Oversee implementation of the Defense security framework.

d. Approve the strategic plan and monitor its execution.

e. Commission reviews and in-depth studies of security issues and, based on the results, make recommendations for developing or improving policies, processes, procedures, and products to address pervasive, enduring, or emerging security challenges.

f. Review resource investments and priorities and recommend changes to the Defense security program to the USD(I), through the Defense Security Executive.

g. Provide a forum for identification, documentation, and dissemination of best practices, including those associated with security risk management.

h. Identify performance measures to be used to assess the effectiveness of the Defense security program and its contribution to mission success.

2. MEMBERSHIP

a. The voting membership of the DSE ExCom shall consist of:

(1) The Defense Security Executive, who shall serve as the Chair.

(2) The DoD Component security program executives designated by the Secretaries of the Military Departments and the Chairman of the Joint Chiefs of Staff in accordance with paragraph 12.e of Enclosure 3 of this Directive.

(3) Representatives of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense (USD(C)/CFO); the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)); the Under Secretary of Defense for Policy (USD(P)); the Under Secretary of Defense for Personnel and Readiness (USD(P&R)); the DoD Chief Information Officer (DoD CIO); the Director of Administration and Management (DA&M); and the General Counsel of the Department of Defense (GC DoD).

(4) Director, DoD SAP Central Office (DoD SAPCO).

(5) Director, Security Directorate, Office of the Deputy Under Secretary of Defense for Intelligence and Security (DUSD(I&S)).

(6) Director, Counterintelligence Directorate, Office of the DUSD(I&S).

b. The Chair may invite representatives from Defense Security Service (DSS) and the Offices of the Inspector General of the Department of Defense and the DNI and others as appropriate to participate as non-voting members of the DSE ExCom.

c. Additional voting members may be added, as necessary, upon recommendation to and agreement of the DSE ExCom.

3. MEETINGS. The DSE ExCom shall meet no less than semiannually and as required at the call of the Chair. The Chair shall set the agenda with input from the members.

4. SUBGROUPS AND WORKING GROUPS. The DSE ExCom may establish such standing subgroups or ad-hoc working groups as deemed necessary. Each group shall have a charter or specific tasking document. Meeting minutes shall be maintained and agreed to by the members of the subgroup or working group and action items shall be tracked. Copies of minutes and action items shall be provided to the executive secretariat for tracking on behalf of the DSE ExCom. Reports of progress or action shall be provided to the DSE ExCom as requested, but no less than annually.

5. ADMINISTRATION

a. The Director, Security Directorate, Office of the DUSD(I&S), shall be the executive secretary and shall arrange meetings; prepare, coordinate, and publish minutes; track action items; and perform other duties as the Chair or DSE ExCom may assign.

b. The DSE ExCom shall establish procedures for its operation and that of the subgroups or working groups, as needed.

ENCLOSURE 3
RESPONSIBILITIES

1. USD(I). The USD(I) shall:

a. Exercise security responsibilities as described in Reference (b), to include serving as the DoD senior official reporting to the Secretary and Deputy Secretary of Defense for development and integration of risk-managed security policies and programs. In carrying out these responsibilities, the USD(I) shall:

(1) Report to and advise the Secretary of Defense on the security implications of strategic planning decisions and on other significant issues raised by the Defense Security Executive or DSE ExCom.

(2) Oversee Defense security policy, plans, programs, and resources and ensure that security policies and programs are designed and managed to improve standards of performance, economy, and efficiency.

b. Coordinate with USD(AT&L), USD(P), and DoD CIO, as appropriate, to establish DSE policy, procedures, and investment goals that align with those established for nuclear physical security, information assurance, foreign disclosure, security cooperation, technology transfer, export control, cyber security, antiterrorism, force protection and mission assurance, and are informed by other security-related efforts (e.g., critical infrastructure protection, insider threat initiatives).

c. Coordinate with the USD(P&R) to ensure DSE policy, procedures, and investment goals are harmonized with personnel policy and procedures.

2. DUSD(I&S). The DUSD(I&S), under the authority, direction, and control of the USD(I), shall serve as the Defense Security Executive and fulfill the responsibilities identified in Enclosure 4 of this Directive.

3. DIRECTOR, DSS. The Director, DSS, consistent with DoDD 5105.42 (Reference (e)) and under the authority, direction, and control of the USD(I), in addition to the responsibilities in section 12 of this enclosure, shall:

a. Provide input, as requested by the Defense Security Executive or DSE ExCom, for the development of the Defense security framework and strategic plan.

b. Establish security education, training, certification, and professional development programs that are integrated with the DSE policy, procedures, and investment goals.

4. USD(AT&L). The USD(AT&L), consistent with DoDD 5134.01 (Reference (f)) and in addition to the responsibilities in section 13 of this enclosure, shall:

- a. Appoint a representative at the general or flag officer level (or Senior Executive Service (SES) equivalent) to serve on the DSE ExCom.
- b. Assist with development of the Defense security framework and strategic plan.
- c. Provide advice, as may be necessary or requested, to the Defense Security Executive and the DSE ExCom within assigned areas of responsibility, including procurement policy and Defense Industrial Base implementation.

5. DIRECTOR, DoD SAPCO. The Director, DoD SAPCO, administratively supported by the USD(AT&L) and reporting to the Deputy Secretary of Defense, shall, consistent with DoDD 5205.07 (Reference (g)):

- a. Serve on the DSE ExCom.
- b. Assist with development of the Defense security framework and strategic plan and coordinate on SAP security policy developed by a working group overseen by the DSE ExCom.

6. USD(P). The USD(P), consistent with DoDD 5111.1 (Reference (h)) and in addition to the responsibilities in section 13 of this enclosure, shall:

- a. Appoint a representative at the general or flag officer level (or SES equivalent) to serve on the DSE ExCom.
- b. Assist with development of the Defense security framework and strategic plan.
- c. Provide advice, as may be necessary or requested, to the Defense Security Executive and the DSE ExCom on security policy issues as they pertain to countering weapons of mass destruction programs; technology security policies on international transfers of defense-related goods, services, and technologies; and global security cooperation programs.

7. USD(P&R). The USD(P&R), consistent with DoDD 5124.02 (Reference (i)) and in addition to the responsibilities in section 13 of this enclosure, shall:

- a. Appoint a representative at the general or flag officer level (or SES equivalent) to serve on the DSE ExCom.
- b. Provide advice, as may be necessary or requested, to the Defense Security Executive and the DSE ExCom on civilian and military personnel issues, including those related to position

sensitivity designation, performance standards, evaluation criteria, and alignment of suitability matters in accordance with Joint Security and Suitability Reform Team initiatives.

c. Assist with development of the Defense security framework and strategic plan.

8. USD(C)/CFO. The USD(C)/CFO, consistent with DoDD 5118.03 (Reference (j)) and in addition to the responsibilities in section 13 of this enclosure, shall:

a. Appoint a representative at the general or flag officer level (or SES equivalent) to serve on the DSE ExCom.

b. Provide advice, as may be necessary or requested, to the Defense Security Executive and the DSE ExCom on issues related to security funding, costing, and performance measures.

9. DoD CIO. The DoD CIO, consistent with DoDD 5144.1 (Reference (k)) and in addition to the responsibilities in section 13 of this enclosure, shall:

a. Appoint a representative at the general or flag officer level (or SES equivalent) to serve on the DSE ExCom.

b. Assist with development of the Defense security framework and strategic plan and shall coordinate with the USD(I) to establish information assurance policy that aligns with the DSE policy, procedures, and investment goals.

10. GC DoD. The GC DoD, consistent with DoDD 5145.01 (Reference (l)) and in addition to the responsibilities in section 13 of this enclosure, shall:

a. Appoint a representative at the general or flag officer level (or SES equivalent) to serve on the DSE ExCom.

b. Provide legal advice and counsel, as may be necessary or requested, to the Defense Security Executive and the DSE ExCom.

11. DA&M. The DA&M, consistent with DoDD 5105.53 (Reference (m)) and in addition to the responsibilities in section 13 of this enclosure, shall appoint a representative at the general or flag officer level (or SES equivalent) to serve on the DSE ExCom.

12. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components, who have overall authority and responsibility for implementation and execution of the security program within their organizations, shall:

a. Ensure that DoD security policies and guidance are implemented.

b. Promote proactive, informed execution of security requirements within their Component, predicated upon the premise that security is everyone's responsibility on a day-to-day basis, and provide oversight to confirm that all Component personnel understand their roles and responsibilities in ensuring DoD security.

c. Establish programs to hire, train, and retain a professional security workforce consistent with this Directive, DoD Instruction 3305.13 (Reference (n)), and Reference (c).

d. Align the DoD Component's security investment portfolio with the DSE policies and guidance.

e. Designate a single DoD Component security program executive, at the general or flag officer level (or SES equivalent), who shall:

(1) Have knowledge of the security disciplines within the DSE necessary to facilitate and oversee implementation of the Defense security framework and strategic plan and the requirements of this Directive within the Component. (This Directive does not affect the ability of the Head of the DoD Component to designate separate officials to direct and oversee specific security functions or disciplines.)

(2) Provide leadership for and maintain cognizance over the Component's process for resourcing its security program, to ensure adequate investment of resources to support an integrated security program, and provide information on those efforts as requested by the Defense Security Executive.

(3) Share cost, schedule, and performance data regarding the DoD Component's security program and investments with the DSE ExCom as needed for execution of its responsibilities.

f. Designate qualified personnel for sub-groups when requested by the DSE ExCom (with the exception of the Office of the Inspector General of the Department of Defense, which conducts and supervises audits and investigations relating to the programs and operations of the DoD in accordance with DoDD 5106.01 (Reference (o))).

13. HEADS OF THE OSD COMPONENTS. The Heads of the OSD Components, according to their responsibility and authority for assigned functional areas, shall:

a. Ensure that DoD security policies and guidance are implemented.

b. Promote proactive, informed execution of security requirements within their Component, predicated upon the premise that security is everyone's responsibility on a day-to-day basis, and provide oversight to confirm that all Component personnel understand their roles and responsibilities in ensuring DoD security.

c. Establish programs to hire, train, and retain a professional security workforce consistent with this Directive and References (c) and (n).

d. Provide leadership for and maintain cognizance over processes for resourcing Component security programs, to ensure investment of adequate resources for an integrated security program, foster alignment of the Component's security investment portfolio with the DSE policies and guidance, and provide information on those efforts as requested by the Defense Security Executive.

e. Share cost, schedule, and performance data regarding the OSD Component's security program and investments with the DSE ExCom as needed for execution of its responsibilities.

f. Designate qualified personnel for sub-groups when requested by the DSE ExCom.

ENCLOSURE 4

DEFENSE SECURITY EXECUTIVE

The Defense Security Executive, under the authority, direction, and control of the USD(I) and consistent with Reference (b), shall:

a. Develop policy and an integrated Defense security framework and strategic plan for the management and oversight of the DSE and in that role shall:

(1) Be responsible for cross functional security coordination.

(2) Report to and advise the USD(I) on the security implications of strategic planning decisions and on other significant issues, including those identified or raised by the DSE ExCom.

(3) With the advice and coordination of the DSE ExCom, develop, maintain, and implement an integrated, cohesive Defense security framework and strategic plan; establish performance measures to assess implementation; and provide oversight to ensure compliance. In executing this responsibility, the Defense Security Executive shall:

(a) Coordinate with the DSE ExCom in the development of an integrated security framework for the DSE and when recommending security policy and procedures to facilitate its implementation.

(b) Ensure the Defense security framework includes provisions for access to integrated education, training, and professional experience opportunities for security professionals, in accordance with Executive Order 13434 (Reference (p)) and References (c) and (n); and to security awareness training for all DoD personnel.

(c) Provide guidance on, and a methodology for, use of the Defense security framework to facilitate tracking security costs, estimating future years resource requirements, measuring return on security investments, and making risk-managed decisions regarding use of security resources.

(d) Develop, coordinate, maintain, and implement a strategic plan that describes how the integrated security framework and the activities, functions, and processes required for its execution will be implemented and measured to support accomplishment of the DoD mission.

b. On behalf of the USD(I), propose DoD resource programs, formulate budget estimates, recommend resource investments and priorities, and monitor the implementation of approved programs in order to ensure adherence to approved security policy and planning guidance.

c. Provide oversight of the DSE and the individual constituent security disciplines, with a focus on identifying opportunities for increased standardization and improved performance, effectiveness, and efficiency.

- d. Chair the DSE ExCom.

- e. Collaborate with the DNI and other external organizations responsible for the development and implementation of national security policy and raise appropriate issues to the DSE ExCom for their consideration.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

DA&M	Director of Administration and Management
DNI	Director of National Intelligence
DoD CIO	DoD Chief Information Officer
DoD SAPCO	DoD SAP Central Office
DoDD	DoD Directive
DSE	Defense Security Enterprise
DSE ExCom	Defense Security Enterprise Executive Committee
DSS	Defense Security Service
DUSD(I&S)	Deputy Under Secretary of Defense for Intelligence and Security
GC DoD	General Counsel of the Department of Defense
SAP	special access program
SES	Senior Executive Service
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Directive.

antiterrorism. Defined in Joint Publication 1-02 (Reference (q)).

controlled unclassified information. Unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable laws, regulations, Executive orders, and Government-wide policies.

Defense Security Executive. The official under USD(I) authority, direction, and control who has responsibility for policy development and oversight of the DSE. DUSD(I&S) is designated to be the Defense Security Executive.

Defense security framework. Structure or architecture describing how security disciplines relate to and interact with each other.

Defense security program. The programmatic planning, expenditures, and return on investment estimating process for the DSE.

DoD Component security program executive. The designated individual with responsibility for and authority to accomplish security program objectives for development, production, and sustainment to meet the user's operational needs. The security program executive shall be accountable for credible cost, schedule, and performance reporting to the Defense Security Executive.

DSE. The organizations, infrastructure, and measures (to include 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, and chemical and biological security, as well as SAP security policy, critical program information 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 counterintelligence, information assurance, foreign disclosure, security cooperation, technology transfer, export control, cyber security, nuclear physical security, antiterrorism, force protection, and mission assurance policy and is informed by other security related efforts.

heads of the Intelligence Community elements. Heads of elements or agencies of the U.S. Government identified in or designated pursuant to section 401a(4) of title 50, United States Code (Reference (r)) or section 3.5(h) of Reference (a).

industrial security. A multi-disciplinary security program concerned with the protection of classified information developed by or entrusted to U.S. industry.

information. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that is owned by, produced by or for, or is under the control of the U.S. Government.

information assurance. Defined in DoDD 8500.01E (Reference (s)).

information security. The security discipline concerned with implementation of a system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure information that is authorized protection by Executive order, statute, or regulation. Information security includes protection of classified, controlled unclassified, and sensitive compartmented information.

insider threat. A person with authorized access who uses that access, wittingly or unwittingly, to harm national security interests and/or national security through unauthorized disclosure, data

modification, espionage, terrorism, or kinetic actions resulting in the loss or degradation of resources or capabilities.

operations security. A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to:

Identify those actions that can be observed by adversary intelligence systems.

Determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical intelligence in time to be useful to adversaries and determine which of these represent an unacceptable risk.

Select and execute countermeasures that eliminate or reduce to an acceptable level the risks to friendly actions and operations.

personnel security. The security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information or assignment in sensitive positions.

physical security. The security discipline concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

professional security workforce. Workforce comprised of security professionals.

SAP. A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

security. Proactive measures adopted to safeguard personnel, information, operations, resources, technologies, facilities, and foreign relations against harm, loss, or hostile acts and influences.

security professional. An individual who is educated, trained, and experienced in one or more security disciplines and provides advice and expertise to senior officials on the effective and efficient implementation, operation, and administration of the organization's security programs.

sensitive compartmented information. Classified national intelligence concerning or derived from intelligence sources, methods, or analytical processes that is required to be protected within formal access control systems established and overseen by the DNI.