Director of Administration and Management

ADMINISTRATIVE INSTRUCTION

NUMBER 56
April 29, 2013

DA&M

SUBJECT: Management of Information Technology (IT) Enterprise Resources and Services for OSD, Washington Headquarters Services (WHS), and Pentagon Force Protection Agency (PFPA)

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5105.53 (Reference (a)), this administrative instruction (AI):

a. Reissues AI 56 (Reference (b)) to implement DoD policy as described in section 3 and to establish centralized management of Enterprise IT programs and services pursuant to the Secretary of Defense Memorandum (Reference (c)).

b. Assigns responsibilities and establishes oversight for management, planning, budgeting, acquisition, and lifecycle management of Enterprise IT resources in accordance with chapter 113 of Title 40, United States Code (U.S.C.) (also known and referred to in this AI as "The Clinger-Cohen Act" (Reference (d))), DoDD 8000.01 (Reference (e)), and Office of Management and Budget (OMB) Circular A-130 (Reference (f)).

c. Assigns responsibility for ensuring the security of information networks in accordance with Title 44, U.S.C. (section 3541 et. seq. of Title 44, U.S.C., is also known as "The Federal Information Security Management Act of 2002" (Reference (g)) and DoDD 8500.01E (Reference (h)).

2. APPLICABILITY

a. This AI applies to OSD, WHS, PFPA, and other DoD organizations that receive IT support and services from the Enterprise IT Services Directorate (EITSD), WHS, (referred to collectively in this AI as the "WHS-serviced Components"), in accordance with Reference (a).

b. Nothing in this AI prevents the Inspector General of the Department of Defense from fulfilling his or her duties pursuant to Title 5, U.S.C. Appendix (also known as "The Inspector General Act of 1978," as amended (Reference (i))).

3. POLICY. It is WHS policy that:

a. In accordance with References (c) through (h), IT acquisition, resources, and services for DoD will be consolidated and centrally planned and managed to provide effective IT services to end-users and their organizations, eliminate redundant and outdated systems, manage risk, maximize information security, promote interoperability, protect privacy in accordance with DoDD 5400.11 (Reference (j)), and ensure continuity of services in accordance with DoDD 3020.26 (Reference (k)).

b. Investments in information systems are managed through a capital planning and investment control process based on performance and results to meet the mission and business requirements of the WHS-serviced Components in accordance with Reference (d).

c. Information systems comply with DoD architecture, information sharing, standards, and policy requirements in accordance with Reference (e).

d. Mission-essential information systems are accessible in emergency contingencies from alternate locations in accordance with Reference (k).

e. Information systems comply with:

(1) Item identification and item level traceability in accordance with DoD Instruction (DoDI) 8320.04 (Reference (l)).

(2) Property accountability requirements in accordance with DoDI 5000.64 (Reference (m)).

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. **Unlimited**. This AI 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 AI:

a. Is effective April 29, 2013.

b. Must be reissued, cancelled, or certified current within 5 years of its publication in accordance with DoDI 5025.01 (Reference (n)). If not it will expire effective April 29, 2023 and be removed from the DoD Issuances Website.

Michael L. Rhodes
Director of Administration and Management

Enclosures
1. References
2. Responsibilities
3. Procedures
4. OSD CIO Roles and Responsibilities
5. EITSD Director Roles and Responsibilities

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5105.53, "Director of Administration and Management (DA&M)," February 26, 2008
(b) Administrative Instruction No. 56, "Automated Information Resource Management (AIRM) in the Office of the Secretary of Defense (OSD) and the Washington Headquarters Services (WHS)," August 20, 1991 (hereby cancelled)
(c) Secretary of Defense Memorandum, "Track Four Efficiency Initiatives Decision," March 14, 2011
(d) Chapter 113 of Title 40, United States Code (also known as "The Clinger-Cohen Act")
(e) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009
(f) Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," November 3, 2003
(g) Title 44, United States Code
(h) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
(i) Title 5, Appendix, United States Code, as amended (also known as "the Inspector General Act of 1978")
(j) DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007, as amended
(k) DoD Directive 3020.26, "Department of Defense Continuity Programs," January 9, 2009
(l) DoD Instruction 8320.04, "Item Unique Identification (IUID) Standards for Tangible Personal Property," June 16, 2008
(m) DoD Instruction 5000.64, "Accountability and Management of DoD Equipment and Other Accountable Property," May 19, 2011
(n) DoD Instruction 5025.01, "DoD Directives Program," September 26, 2012
(o) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007
(p) Office of the Secretary of Defense IT Board of Directors Charter, OSD 00746-09, February 3, 2009
(q) DoD Directive 5110.04, "Washington Headquarters Services (WHS)," March 27, 2013
(r) Federal Acquisition Regulation, current edition
(s) Subpart 211.274 of the Defense Federal Acquisition Regulation Supplement, current edition
(t) DoD Directive 5105.68, "Pentagon Force Protection Agency (PFPA)," December 19, 2008
(u) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008, as amended
(v) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended
(w) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010
(x) DoD Instruction 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)," February 6, 2013
(y) Section 131, Title 10, United States Code

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR OF ADMINISTRATION AND MANAGEMENT (DA&M). The DA&M:

a. Provides policy, oversight, direction, and control of information resources, systems, printing services, remote and wireless communications, and telephone communications systems management for the WHS-serviced Components and supported OSD facilities in the National Capital Region, including alternate sites in accordance with References (a), (c) through (h), and DoDI 8510.01 (Reference (o)).

b. Appoints an OSD Chief Information Officer (OSD CIO) who, for WHS-serviced Components and in cooperation with the OSD IT Board of Directors (OSD IT BOD), which is chartered in Reference (p), executes the roles and responsibilities delineated in Enclosure 4 of this AI.

2. DIRECTOR, WHS. Under the authority, direction, and control of the DA&M, and in accordance with the authority in DoDD 5110.4 (Reference (q)), the Director, WHS:

a. Provides Enterprise-wide IT business solutions to support WHS-serviced Component missions.

b. Oversees the execution of roles and responsibilities of the Director, EITSD, as delineated in Enclosure 5.

3. WHS-SERVICED COMPONENTS HEADS. The WHS-serviced Component heads:

a. Complete and provide the documentation needed for Enterprise IT investments.

b. Participate in developing IT requirements and acquisition documentation, including development of requirements support for independent government cost estimates.

c. Develop and manage mission applications for respective functional areas by:

(1) Providing periodic updates on those applications to the OSD IT BOD.

(2) Establishing requirements and managing content and data for component mission applications.

(3) Nominating component applications for consideration as Enterprise solutions.

d. Specify performance and delivery requirements for systems and support services.

e. Participate in IT project in-progress reviews.

f. Review for completeness and accuracy all IT systems compliance submissions pursuant to Reference (e).

g. Develop evaluation criteria and participate in IT contract source selection panels.

h. Provide required information to designated IT contracting officer's representatives overseeing IT contracts, reports, invoices, and documentation of goods received or services performed.

i. If justification and approval is required for other than full and open competition, provide to EITSD the information that supports the justification and approval in accordance with Federal Acquisition Regulations (Reference (r)).

j. Assist in the preparation of business case analyses and performance assessments to maximize the benefits derived from organizational IT capital asset investments and support the development of IT capital asset strategies, plans, budgets, acquisition strategies, and use.

k. Program and budget for unique organizational IT business capabilities in coordination with the WHS IT service provider and in accordance with Reference (q).

l. Obtain approval from the Director, WHS, and concurrence from Director, Acquisitions Directorate, WHS, before seeking IT services through an organization other than the WHS contracting office.

m. Execute DoD data management strategy.

n. Collaborate with EITSD to prioritize helpdesk workload to align with component mission, operational needs, and Enterprise IT initiatives.

o. Nominate procedures for standard operating procedures (SOPs) development.

ENCLOSURE 3

PROCEDURES

1. REQUESTING SERVICES. WHS-serviced Component users will submit requests for IT services, telecommunications services, new or replacement equipment, office move assistance, and any other IT or telecommunications services through the helpdesk. For purchase of IT equipment, procurement requests will be submitted through the automated Remedy request system.

2. REQUESTS FOR IT EQUIPMENT PURCHASES. WHS-serviced Components requesting purchases of IT equipment, software, supplies, and support services above the micro-purchase threshold must provide a performance work statement, salient characteristics, or a similar specification sufficient to make the purchase in accordance with subpart 211.274 of the Defense Federal Acquisition Regulation Supplement (Reference (s)). Micro-purchases must follow IT configuration standards established by EITSD and, when appropriate, be established on the WHS accountable property system of record in accordance with Reference (m).

3. LOST OR STOLEN EQUIPMENT. The user, custodian, and security manager will report lost or stolen IT equipment.

a. User Responsibility. WHS-serviced Component users of government-furnished IT equipment must immediately notify their supervisors and security managers of the loss of an IT asset. If the asset is lost or stolen inside a WHS-serviced facility, the user's security manager must immediately notify PFPA, which provides law enforcement for the Pentagon Reservation and for assigned DoD activities and DoD-occupied facilities within the National Capital Region as part of the PFPA mission in accordance with DoDD 5105.68, (Reference (t)). For assets lost or stolen in public jurisdictions, the user must immediately contact local police to report the loss or theft and, as soon as possible, provide their security manager with a copy of the local police report. The security manager will provide the police report to PFPA, which maintains liaison with local police authorities. The user must provide copies of all written reports to the custodian of the missing asset.

b. Custodian Responsibility. The custodian will provide all available information about the item and the incident to the appropriate WHS-serviced Component security manager and deactivate all security-enabled services. The custodian must also provide relevant supporting documentation to the accountable property officer to ensure an auditable trail for equipment meeting accountability requirements in accordance with Reference (m).

c. Security Manager Responsibility. The WHS-serviced Component security manager will conduct a full investigation, maintain a case file for each asset reported as lost or stolen, provide a copy of the police report to PFPA, and engage with the EITSD security manager once the investigation begins. If the lost or stolen equipment contains classified information, other

component security managers will be notified as necessary. If the equipment contains controlled unclassified information (which includes personally identifiable information (PII)), the security manager will notify the agency responsible for the information. Lost or stolen PII incidents must be reported to the Component Privacy Office in accordance with Reference (j).

4. REPORTING DATA SPILLS

a. All personnel who have knowledge of confirmed or suspected incidents of failure to properly safeguard classified information must immediately notify their Component Security Manager.

b. When classified information is transferred to information systems, applications, or media of lower classification, in addition to the Component Security Manager, users must notify the EITSD service desk at osdhelpdesk@osd.mil.

c. Spills involving handheld devices may result in the disablement of the device pending erasure of all data on the device, including emails and contacts. EITSD will ensure devices remain disabled pending the sanitization of the associated email infrastructure.

d. EITSD will ensure, pursuant to DoDI 5200.01 (Reference (u)), DoD Manual 5200.01 Volume 3 (Reference (v)), DoDD 5205.7 (Reference (w)), and DoDI 5205.11 (Reference (x)) that:

(1) Sensitive compartmented information (SCI) and special access program (SAP) data spills result in destruction of the handheld device and issuance of a new device. SCI spills will be reported to the Intelligence Community Incident Response Center and the data owner will respond with appropriate clean-up procedures. SAP spills will be immediately reported to the DoD SAP Central Office for guidance and resolution by appropriately accessed personnel.

(2) All data spills involving email accounts result in disabling the user email accounts for all individuals involved for the duration of the sanitizing of the email infrastructure and workstations.

(3) Data spills involving classified information result in deletion of the information and temporary files from the workstation, and may result in replacement of the workstation hard drive.

5. SOP DEVELOPMENT. EITSD will develop SOPs to be reviewed by the appropriate IT governance councils prior to publication. WHS-serviced Components receiving services from EITSD will comply with SOPs associated with those services.

ENCLOSURE 4

OSD CIO ROLES AND RESPONSIBILITIES

Under the authority, direction, and control of the DA&M, the OSD CIO serves as the principal advisor for the DA&M and Director, WHS, on all IT and information management (IM) matters related to WHS-serviced Components. In this capacity, the OSD CIO:

a. Develops and provides information resource and IT guidance for the WHS-serviced Components to enable missions and ensure compliance with federal and DoD regulations and policies that govern management, acquisition, interoperability, and security of IT and information systems; oversees implementation of guidance consistent with DoD IT and IM policies.

b. Oversees OSD-wide Enterprise IT and IM services and provides guidance on Enterprise IT resources, programs, and budget matters for WHS-serviced Components, including exercising funding control and monitoring budget executions for WHS-serviced Component IT programs in accordance with References (c), (d), and (e).

c. Oversees OSD Enterprise IT and IM contracts, budget formulation and execution, and personnel allocations and selections; oversees all OSD Enterprise IT and IM resources, including funding, personnel, systems, and physical space.

d. Acts as the responsible agent within OSD for ensuring the Enterprise IT and communications fiscal program is up-to-date, and that funds are available to operate the baseline systems. Develops new capabilities and modernizes a portion of the infrastructure each fiscal year.

e. Advises and consults with the OSD principal staff assistants (PSAs) on all Enterprise IT and IM matters and serves as the principal information resources management advisor to senior OSD managers.

f. Coordinates OSD-wide Enterprise IT and IM requirements and secures requirements from OSD PSAs.

g. Oversees Enterprise-wide IT and IM support agreements negotiated and executed by EITSD on behalf of OSD, and establishes service delivery relationships with other IT service providers as appropriate.

h. Develops an integrated applications portfolio and designates material solutions providers.

i. Reviews key business processes in OSD to identify opportunities to use IT to achieve greater Enterprise-wide efficiencies, improve cross-functional processes, and replace stovepipe systems with Enterprise processes and systems.

j. Establishes and sustains a comprehensive management framework for the consolidated OSD information Enterprise.

k. Serves as OSD's Designated Accrediting Authority for all assigned DoD information systems, and manages and oversees an accredited security architecture that protects Enterprise information systems and networks at all classification levels from internal and external threats, in accordance with References (h) and (k). This does not include intelligence or SAP systems covered by other statutes or regulations.

l. Co-chairs the OSD IT BOD with one of the assigned PSA representatives, who will be elected annually by the OSD IT BOD.

m. Establishes priorities to ensure OSD's Enterprise IT/IM program complies with congressional, OMB, and DoD guidance, and ensures resources are acquired, used, and managed consistent with federal and DoD guidance.

n. Develops resource plans for OSD's Enterprise IT/IM and telecommunications programs, including staffing and budgeting.

o. Serves as OSD's cognizant authority for all Federal-level IT and IM compliance and reporting pertaining to OSD's Enterprise IT efforts including, but not limited to, responsibilities delineated in References (d) and (g).

p. Determines how the Enterprise IT systems and networks will be designed, built, implemented, and maintained through effective architectural and planning initiatives. Coordinates OSD's Enterprise architecture, in conjunction with the OSD IT BOD, including an OMB-compliant Enterprise architecture, OSD Enterprise Information Management Plan, OSD Enterprise IT Strategic Plan, OSD Enterprise Information Assurance Strategic Plan, OSD Enterprise IT annual plan, OSD Enterprise IT metrics plan, OSD Enterprise IT portfolio management program, and IT standards responsive to senior OSD leadership.

q. Chairs IT advisory boards, including the OSD IT BOD and the Pentagon Area CIO Council.

r. Performs the roles and responsibilities of OSD's Senior Information Assurance (IA) Official, including managing OSD's corporate IA efforts and providing final determination on IA policy and guidance.

s. Represents OSD in DoD, government, and private sector IT forums.

t. Develops OSD's IT and IM Continuity of Operations, Continuity of Government, and Continuity of Business plans.

u. Oversees lifecycle replacement plans and program and project plans for OSD's Enterprise IT/IM program.

ENCLOSURE 5

EITSD DIRECTOR ROLES AND RESPONSIBILITIES

Under the authority, direction, and control of the Director, WHS, the Director, EITSD:

a. Provides a full spectrum of executive communication capabilities to the OSD for the execution of mission essential functions, including command and control, in all required business locations, regardless of threat environment.

b. Plans, designs, implements, operates, maintains, and funds Enterprise IT solutions that leverage or provide DoD enterprise services using cloud or shared service solutions whenever security and the analysis of alternatives support these approaches.

c. Assists the OSD CIO in developing solutions, plans, and budgets for Enterprise IT systems and support services.

d. Standardizes delivery of state-of-the-art Enterprise IT and telecommunications services.

e. Manages the central architecture, classified and unclassified networks, security, applications, and services for the Enterprise, consistent with chapter 35, subchapter I, section 3506 of Reference (g) and in accordance with Reference (h), and manages and controls changes to the standards-based architecture, operational IT baselines, and configurations.

f. Oversees compliance with information security systems, network security, and IA training requirements.

g. Provides Enterprise IT systems and support services for the DoD Headquarters Continuity of Operations and alternate sites, in accordance with Reference (k).

h. Plans, programs, budgets, and executes an Enterprise-wide IT acquisition program including contract and past performance, and administration through close out, in accordance with References (c), (d), (e), and (f) that:

(1) Consists of standardized IT hardware and computer equipment and uses software acquisition strategies and solutions that maximize effectiveness of IT services to the end-users and their organizations.

(2) Includes business case analyses and performance assessments to maximize the benefits derived from Enterprise-wide IT capital asset investments, and supports the development of IT capital asset plans, budgets, and acquisition strategies in accordance with References (d) and (e) and subparts 8:405-6 and 6.3 of Reference (r).

(3) Establishes an Enterprise IT capital planning and investment control process in accordance with References (d) and (e), and defines, oversees, manages, and reports to the DA&M on the Enterprise IT acquisition process.

(4) Centralizes approval of all purchases of Enterprise IT products and services to ensure compliance with DoD plans and standards.

(5) Establishes, centrally manages, and administers all Enterprise IT contracts to provide cost-effective, consolidated solutions to meet the WHS-serviced Components' IT business requirements for services, equipment, and maintenance.

(6) Provides for item identification and traceability requirements in accordance with References (l), (m), and (s).

(7) Establishes Enterprise IT network and performance goals to drive continuous process improvement across Enterprise-wide IT services; develops effective measurements to show progress toward achieving those goals with the OSD IT BOD.

(8) Ensures all Enterprise IT systems comply with DoD Enterprise Architecture guidelines in accordance with Reference (e).

i. Annually reviews the OSD IT systems portfolio of applications for Enterprise-wide solutions.

(1) Establishes and executes Enterprise lifecycle management for information systems, hardware, software, and license management programs.

(2) Maintains control of and ensures all Enterprise IT assets are recorded in the WHS accountable property system of record in accordance with Reference (m).

j. Provides technical assistance and maintenance support.

(1) Establishes a customer relationship management effort that facilitates access to the IT service provider for expedited delivery of service and problem resolution. This includes forward-deployed assets as appropriate.

(2) Establishes and maintains a repository for Enterprise IT SOPs. The SOPs cover services, support, and hardware and software management pertinent to the daily operations of the IT Enterprise.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AI	administrative instruction
BOD	Board of Directors
CIO	Chief Information Officer
DA&M	Director of Administration and Management
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
EITSD	Enterprise Information Technology Services Directorate
IA	information assurance
IM	information management
IT	information technology
OMB	Office of Management and Budget
PFPA	Pentagon Force Protection Agency
PII	personally identifiable information
PSA	Principal Staff Assistant
SAP	special access program
SCI	sensitive compartmented information
SOP	standard operating procedure
U.S.C.	United States Code
WHS	Washington Headquarters Services

PART II. DEFINITIONS

These terms and their definitions are for the purpose of this AI.

contracting officer's representative. Any individual delegated responsibilities by a warranted contracting officer to make purchases.

custodian. Designated individual responsible for managing all IT property under their purview such as desktop computers, laptops, printers, and scanners.

designated accrediting authority. The official authorized to formally assume responsibility for operating a system or network at an acceptable level of risk.

data spill. A security incident where the transfer of information of a higher classification to information systems, applications, or media of a lower classification, jeopardizes the confidentiality of U.S. Government information.

defense business system. An information system, other than a national security system, operated by, for, or on behalf of the Department of Defense, including financial systems, mixed systems, financial data feeder systems, and IT and IA infrastructure, used to support business activities such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management.

EITSD. A WHS directorate responsible for the day-to-day IT support for OSD, WHS, and PFPA. Provides operational support, central planning, integration, and coordinated execution of the OSD CIO's enterprise-wide programs and projects, and oversight of far-reaching initiatives that impact, or are impacted by, enterprise initiatives and decisions.

Enterprise. A system that has been identified as the standard across the DoD. Enterprise-level, within the context of tiered accountability, refers to programs/solutions managed by OSD. Tiered accountability is an approach to business transformation that is based on dividing the planning and management of programs and initiatives between Enterprise and Component levels.

enterprise services. All IT services provided to the WHS-serviced Components, including application services, project management, helpdesk services, change configuration, and financial management. Excludes Component-specific applications.

external IT service providers. Commercial or government entities that provide critical technical infrastructure and other capabilities directly to WHS-serviced Components. These services are provided through inter-organizational service level agreements or contracts.

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.

IM. The planning, budgeting, manipulating, and controlling of information throughout its life cycle.

in-progress reviews. Periodic cost versus performance assessments of IT projects to ensure the project remains useful to the DoD.

information resources. Information and related resources, such as personnel, equipment, funds, and IT.

information resource management. The process of managing information resources to accomplish OSD goals for integrated support and services; agile and efficient operations; measured performance to inform decision-making, promote efficiency and enable transparency; and attracting and retaining a highly skilled, versatile, and motivated workforce.

IT. Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes computers, laptops, hand held devices, ancillary equipment, software, firmware, telecommunications equipment and services (including support services), procedures, and related resources.

National Capital Region. The geographic area located within the boundaries of the District of Columbia; Montgomery and Prince Georges counties in the State of Maryland; Arlington, Fairfax, Loudoun, and Prince William counties and the City of Alexandria in the Commonwealth of Virginia; and all cities and other units of government within the geographic areas of such District, counties, and city. This area includes the land and physical facilities at the Raven Rock Mountain Complex.

OSD. As provided for in section 131 of Title 10, U.S.C (Reference (y)), includes the Immediate Office of the Secretary and Deputy Secretary of Defense; the Under Secretaries of Defense; the Deputy Chief Management Officer; the General Counsel of the Department of Defense; the Assistant Secretaries of Defense; the Inspector General of the Department of Defense; Assistants to the Secretary of Defense; the OSD Directors and equivalents, who report directly to the Secretary or the Deputy Secretary of Defense, their staffs, and such other staff offices as the Secretary of Defense establishes within the OSD to assist in carrying out assigned responsibilities.

OSD IT BOD. A permanent IT governance council under the DA&M that provides executive oversight of OSD common IT requirements, architecture, policy, services, resource strategies, and investments.

micro-purchase. A government purchase (supplies or services) under the dollar value of $3,000.00 that does not require competition and is normally conducted informally using a credit card held by an authorized cardholder under an established delegation of authority.

PSA. PSAs include the Under Secretaries of Defense; the Deputy Chief Management Officer; the General Counsel of the Department of Defense; the Inspector General of the Department of Defense; and those Assistant Secretaries of Defense, Assistants to the Secretary of Defense, and OSD Directors and equivalents who report directly to the Secretary or Deputy Secretary of Defense. OSD PSAs are also known as the "OSD Component heads."

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.

SCI. Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled exclusively within formal control systems established by the Director of Central Intelligence.

WHS-serviced Components. Organizations that receive IT support services from WHS, which include the OSD Components, WHS and PFPA Directorates, and the WHS-supported Defense Agencies and Field Activities.

user. Any person within the OSD or WHS-serviced Component, including contractors, who operates a government-furnished computer or other device that processes information.