



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

MCO 5230.21
C4 (CIO)
3 Oct 2012

MARINE CORPS ORDER 5230.21

From: Commandant of the Marine Corps
To: Distribution

Subj: INFORMATION TECHNOLOGY PORTFOLIO MANAGEMENT

Ref: (a) SECNAVINST 5230.14
(b) MCO 5400.52
(c) DoD CIO Memo, DoD IT Portfolio Repository (DITPR) and
DoD SIPRNET IT Registry Guidance, August 10, 2009
(d) MCO 5231.3
(e) SECNAV M-5210.1

Encl: (1) Mission Area Leads, Functional Areas and Functional
Area Managers
(2) Definitions

1. Situation

a. References (a) through (e) provide policy and guidance for implementing Department of Defense (DoD) Information Technology (IT) Portfolio Management (PfM). Reference (a) establishes the overall policy for Department of the Navy (DON) applications and data management, and roles and responsibilities for Functional Area Managers (FAMs), FAM Leads, and Functional Data Managers (FDMs). Reference (a) describes an IT portfolio as a collection of IT investments by capability to accomplish a specific outcome. Portfolios include, but are not limited to, related resources and investments, networks, systems, applications, Commercial-Off-The-Shelf (COTS) and Government-Off-The-Shelf (GOTS) solutions.

b. PfM within the Federal Government is a fundamental business imperative. As the demand for additional capabilities increases and resources become more constrained, PfM provides a means to eliminate duplication while prioritizing and validating requirements. In addition to advocating resources and requirements, PfM will support increased and enhanced net-

DISTRIBUTION STATEMENT A: Approved for public release;
distribution is unlimited

centricity, interoperability, information assurance (IA), and knowledge management (KM) as per references (a) through (e).

c. All military departments and defense agencies are required to implement IT PFM in order to provide a balanced strategy for making decisions and recommendations based on enterprise strategic planning, integrated architectures, and capability-based performance. IT portfolio alignment by Functional Areas (or capabilities) aligns IT investments with the needs of the warfighter, intelligence and business activities that support the warfighting functions, and provides a method to categorize, understand, and manage Marine Corps IT portfolios.

2. Cancellation. MARADMINs 226/04, 287/06, and 253/11.

3. Mission

a. This Order promulgates Marine Corps policy for IT PFM and provides guidance on IT capability management and investment decision-making; defines roles and responsibilities for personnel implementing IT PFM; and provides references to enhance support of key IT PFM decision-makers per the Director, Command, Control, Communications, and Computers Department (Dir C4)/DON Deputy Chief Information Officer, Marine Corps (DDCIO(MC)) and references (a) through (e).

b. To ensure IT investments support the Marine Corps vision, strategy, mission, and goals; facilitate efficient and effective delivery of capabilities to the warfighter; and maximize return on investment, this Order:

(1) Establishes Marine Corps IT PFM as the primary process to support IT capability management and investment decisions.

(2) Establishes the roles and responsibilities of Marine Corps Mission Area Leads (MALs), FAMs, FAM Leads, FDMs, and Program Managers (PMs).

(3) Enhances the ability of key decision-makers to assess the probable impact of IT investments on operational performance by demonstrating the relationships among current and planned investments.

4. Execution

a. Commander's Intent

(1) Marine Corps IT portfolios consist of 13 Marine Corps and 6 Secretary of the Navy (SECNAV)/Chief of Naval Operations (OPNAV) Functional Areas, listed in enclosure (1).

(2) Marine Corps IT portfolios as listed in the DoD Information Technology Portfolio Repository - DON (DITPR-DON) and the DON Application and Database Management System (DADMS) are the authoritative listing of all systems and applications approved by FAMs and the Dir C4/DDCIO(MC) for use within the Marine Corps. Marine Corps IT portfolios are a collection of COTS, GOTS, and joint systems/applications used within the Marine Corps Information Enterprise (MCIENT).

(a) Per reference (c), the Office of the Secretary of Defense (OSD) has mandated the use of DITPR as the authoritative unclassified inventory of IT systems. DON CIO implemented use of DITPR-DON as the DON source for collecting required IT data and uploading it to the DITPR. This requirement includes National Security Systems (NSS) system data.

(b) DITPR-DON provides unclassified information on DON IT systems to DITPR after appropriate levels of review and approval in accordance with reference (c) and annual DITPR-DON guidance published by DON CIO. DITPR-DON meets all of the requirements established for DITPR. Per reference (a), IT systems shall be registered in DITPR-DON. DON CIO registration guidance is the authoritative source for information on actions required to meet the registration requirement. DITPR-DON registration guidance is available for download at www.doncio.navy.mil.

(c) DADMS is the Authoritative Data Source (ADS) for DON IT and NSS applications and database inventory, and requires databases and applications to be registered in DADMS. DON CIO registration guidance is the authoritative source for information on actions required to meet the registration requirements. DADMS registration guidance is available for download at www.doncio.navy.mil.

(d) Per reference (d), the Marine Corps ADS Directory is the authoritative source for all Marine Corps ADSs.

The Directory provides the listing, description, and ownership assignment for all ADSs. FAM Leads will designate ADS within their portfolios and register (as well as maintain the accuracy of) them in the Marine Corps ADS Directory. ADS Directory registration guidance is located at

<https://ehqmc.usmc.mil/sites/itsg/ncds/default.aspx>.

(e) Enclosure (2) provides specific definitions of an application, system, database and ADS.

(3) Deputy Commandants (DC), Directors (Dir), and Commanding Generals (CG) are designated as the FAMs. Organizations/commands designated the responsibility for executing FAM and FDM responsibilities for their portfolios are listed in enclosure (1).

b. Concept of Operations

(1) Dir C4/DDCIO(MC) Roles and Responsibilities. As Dir C4/DDCIO(MC) and per references (a) and (b), Dir C4/DDCIO(MC) shall:

(a) Promote net-centricity, interoperability, IA, KM and provide the over-arching IT strategy and goals within the Marine Corps.

(b) Serve as the Marine Corps IT Portfolio Lead for Marine Corps IT portfolios and establish Marine Corps IT PFM policy, processes, guidance and oversight.

(c) Facilitate proper use of DITPR-DON and DADMS.

(d) Ensure accurate IT inventories are maintained and certify annual reviews of all IT systems registered in DITPR-DON per DON Information Management/Information Technology (IM/IT) Investment Review Process Guidance and DON CIO DITPR-DON Registration Guidance.

(e) Chair the USMC IT Steering Group (ITSG), which conducts the IT capital planning and investment process for the Marine Corps and is responsible for assessing Program Objective Memorandum (POM) and non-POM IT initiatives, solutions and investments. The ITSG shall also address potential conflicts concerning Program and IT PFM processes and practices.

3 Oct 2012

(f) Establish measurable performance-based and results-based criteria, in support of portfolio assessments and ITSG consideration.

(g) Review and provide recommendations related to IT investments to Program Evaluation Board (PEB) Chairs, via the DC for Programs and Resources, in support of the Marine Corps Program, Planning, Budgeting and Execution process.

(g) Oversee Marine Corps IT acquisition processes, in coordination with Marine Corps Systems Command (MCSC) and DC for Combat Development and Integration (CDI), to include, but not limited to, Joint Capabilities Integration Development System (JCIDS); Business Capability Lifecycle (BCL); Planning, Programming, Budget and Execution (PPBE); Investment Review Boards (IRBs); the applicable force development system, and IT Procurement Request Review/Approval System (ITPRAS).

(i) Participate in Federal, DoD and DON PFM initiatives to include Federal Enterprise Architecture, Business Enterprise Architecture, and Capabilities PFM.

(2) MAL Roles and Responsibilities

(a) MALs are identified in enclosure (1).

(b) Establish a core set of criteria for managing the respective mission areas.

(c) Ensure portfolio investments meet validated requirements of the mission area.

(d) Coordinate and collaborate with FAMs to identify mission area priorities and requirements, and resolve discrepancies pertaining to investments misaligned within a mission area.

(3) FAM Roles and Responsibilities

(a) FAMs are identified in enclosure (1).

(b) Manage IT Portfolios by implementing and maintaining interoperable, cost effective, and secure IT capabilities and resources driven by Marine Corps mission requirements and aligned with DON, DoD, and Marine Corps mission area strategies.

1. Coordinate the analysis and evaluation of systems, applications, databases, and networks within their portfolio to identify and validate capability gaps, and to eliminate unnecessary or duplicate capabilities in support of improved organizational performance, business activities and warfighting processes.

2. Oversee the initiation, reduction, consolidation, migration, and/or retirement of IT systems, applications, and databases in coordination with PMs and applicable stakeholders and consistent with the respective lifecycle plans, references (a) through (e), and other applicable Marine Corps processes and guidance.

(c) Manage changes to systems, system interfaces, data transfers, ADSs and ADS interactions in coordination with MCSC, DC CDI and/or other appropriate stakeholders to optimize the total IT value of all systems within their portfolios.

(d) Establish FAM level IT PFM processes, and portfolio specific criteria and performance metrics, using the Enterprise and MAL criteria as a baseline. To enhance decision-making on IT investments and per reference (a), IT PFM processes shall be comprised of the following core activities.

1. Analysis. Determine strategic direction for functional area activities and processes; establish portfolio goals linked to the DoD, DON and MCIENT vision, goals, objectives, priorities, and capabilities; identify how these will be achieved, measured and provide for continuous process improvement.

2. Selection. Identify the best mix of IT investments to achieve outcome goals and plans, as well as transition to "to-be" architecture.

3. Control. Provide oversight, direction and guidance to PMs to ensure the systems, applications and individual projects are in accordance with performance and risk baselines and documented technical criteria. These criteria should remain consistent with the current approved version of the Global Information Grid (GIG) Integrated Architecture.

4. Evaluation. Routinely and systematically assess and measure actual contributions of the portfolio as

well as support adjustments to the mix of portfolio projects as necessary.

(e) Ensure that the procedures and certification of business systems with funding over \$1 million dollars across the future years defense plan complies with all applicable requirements.

(f) Ensure all IT systems, applications, and databases within their portfolio are properly registered in DADMS or DITPR-DON. Only those systems, applications and databases that are properly registered per this Order and reference (a) shall be considered for new and/or continued funding.

(g) Appoint a FAM Lead for their portfolio to assume the daily roles and responsibilities of the FAM. The FAM is responsible for clearly identifying the responsibilities and authority of the FAM Lead through a FAM Lead designation letter. A copy of all designation letters shall be forwarded to DIR C4/DDCIO(MC) and validated by the FAMs on a bi-annual basis. FAMs shall notify Dir C4/DDCIO(MC) when FAM Lead personnel transition by submitting new designation letters.

(g) Ensure designated FAM Leads are properly trained to perform FAM Lead functions.

(i) Appoint an FDM to manage and provide oversight for the data within their portfolio. The FAM is responsible for clearly identifying the responsibilities and authority of the FDM through an appointment letter, and to ensure designated FDMs are properly trained to perform FDM functions.

(j) Support their respective MAL and the Dir C4/DDCIO(MC) by integrating IT PFM into their requirements, funding, procurement/acquisition and policy processes. FAMs shall submit funding requirements for their portfolios through, and exercise portfolio investment control during, the PPBE.

(4) FAM Lead Roles and Responsibilities

(a) Work with capabilities integration officers, PMs and Subject Matter Experts (SMEs) to consolidate and enhance IT portfolios.

(b) Provide disposition recommendation for all non-weapon system IT Procurement Requests (ITPRs) (hardware,

software, peripherals, network infrastructure, contract services, etc.) pertaining to new/existing systems and applications funded with Marine Corps appropriations regardless of cost. ITPRs will be processed, reviewed, and approved using ITPRAS which is available at <https://itprocurement.hqi.usmc.mil>. FAM Leads must ensure that technology solutions are aligned with the Marine Corps Enterprise Network and MCIENT Strategy.

(c) Work with PMs, IA Managers, and Product Groups (PG) to complete registration of systems, applications and databases, as defined in enclosure (2), within their portfolio.

(d) Maintain DADMS, DITPR-DON and Marine Corps ADS Directory dispositions of systems, applications, and/or databases. To maintain accuracy and completeness, FAM Leads shall review the registries of all systems, applications and databases at least once annually. Per DON CIO Investment Review Process Guidance, FAM Leads shall ensure all systems registered in DITPR-DON are formally assessed annually as follows:

1. Business Mission Area (BMA) and Enterprise Information Environment Mission Area (EIEEMA) system reviews for DON Enterprise Architecture (EA) compliance must be completed no later than (NLT) 15 February of each year. Overall system reviews shall be completed NLT 15 April of each year.

2. DON EA for systems within the Warfighting and DON Intelligence Mission Areas (DIMA) must be reviewed NLT 15 May of each year. Full system reviews shall be completed NLT 15 July of each year.

3. System registrations are subject to certification by Dir C4/DDCIO(MC) and will be rejected if entries are found to be incomplete and/or non-compliant with one or more applicable policies. Rejected reviews will be at risk for reduced or loss of funding, or recommendation for termination.

4. FAM Leads will provide FAMS with a documented list of system, application, and database entries containing discrepancies. FAM Leads will also provide the respective FAM and Dir C4/DDCIO(MC) with a Plan of Actions and Milestones for correcting the discrepancies.

(e) Per reference (a), FAM Leads shall ensure budget information of their IT investments is registered in Navy IT

Exhibits/Standard Reporting (NITE/STAR). NITE/STAR registration guidance is located at www.doncio.navy.mil and registration shall be coordinated with the DC for Programs and Resources.

(f) Per DoD, DON and Marine Corps investment policies and references (a) and (d), work with IA Managers, PMs and PGs to satisfy the following requirements:

1. Document IT investments and acquisitions.
2. Conduct an annual review and assess performance of the IT portfolio in conjunction with Marine Corps planning and budget processes.
3. Review and update each IT investment and complete a post-implementation review, as well as continuous review of system and/or application changes deemed significant by the FAM Lead.
4. Ensure PMs update DADMS and DITPR-DON to reflect changes in capabilities of IT systems, applications and databases over the previous fiscal year.
5. Ensure IA compliance on all systems and applications, to include compliance with classification, For Official Use Only (FOUO), and Personally Identifiable Information (PII) data processing regulations.

(g) Ensure FDM responsibilities are performed in accordance with the references and other applicable policies and guidelines.

(5) FDM Roles and Responsibilities

(a) Per reference (d), FDMs are responsible for managing data within the Portfolio by supporting the FAM Lead in defining requirements and optimizing availability of required data. FDMs shall coordinate and oversee the identification of ADSs; the reduction of unnecessary, redundant, unsecured or risk-vulnerable databases, data sources and data elements; the consolidation of redundant manual data entry instances; and improving the visibility, accessibility, understandability and reliability of data within the portfolio.

(b) FDMS shall provide guidance and oversight on data requirements from inception of acquisition programs throughout the system and/or data lifecycle.

(c) Work with FAM Leads to develop a portfolio implementation strategy to support the FAMs operational objectives and to satisfy the requirements listed in reference (d) and this Order.

(d) Develop and maintain a data architecture for the portfolio to analyze/capture data flows internal and external to the portfolio and map where data initially enters systems within the portfolio.

(e) Manage data flows within the portfolio and assign data ownership responsibilities for each data source within the portfolio.

(6) PM Roles and Responsibilities

(a) Assist FAM/FAM Leads in maintaining portfolios and ensuring IT requests are not duplicative, are interoperable, net-centric, and in compliance with IA. This shall include, but is not limited to:

1. Providing FAM Leads with project/program status information (i.e., cost, schedule, performance, business case analyses, etc.).

2. Ensuring systems and applications identified for termination are properly terminated.

3. Ensuring disapproved IT procurement requests (to include disapproved requests for applications within DADMS) are not fielded.

(b) Coordinate all requests for IT systems and applications via FAM Leads. All requests for new IT systems and applications, and/or development/modernization of existing systems and applications require FAM concurrence prior to procurement/implementation.

(c) Collaborate with FAMs to properly register new systems and applications in DADMS or DITPR-DON prior to certification and accreditation.

(d) Ensure data in DITPR-DON is kept up-to-date and provide annual PM reviews/assertions prior to due dates listed in paragraph 4b(4) (d) of this Order.

(e) Initiate ITPRs for IT related to new/existing systems and applications. Work with FAM Leads and SMEs to determine whether the requirement represents a valid need and that the requested functionality is not duplicative. When notified by Dir C4/DDCIO(MC) that the ITPR has been reviewed and approved for procurement, PMs are responsible for ensuring approved requirements have been registered in DADMS and/or DITPR-DON.

(7) Commanders

(a) Collaborate with PMs and FAM/FAM Leads to assist in ensuring IT requests are not duplicative, are interoperable, net-centric, and in compliance with IA requirements.

(b) Coordinate all requests for IT systems and applications via FAM Leads and PMs. Ensure systems and applications which are disapproved or identified for termination (to include applications within DADMS that are disapproved, or have not yet been reviewed, by the Marine Corps) are properly terminated or are not fielded.

c. Subordinate Element Missions. The Deputy Commandants for Aviation; Installation and Logistics; Plans, Policies, and Operations; Programs and Resources; Manpower and Reserve Affairs; and Combat Development and Integration; the Dir C4/DDCIO(MC); Director, Intelligence Department (Dir, Intel); and Commanding General, Marine Corps Systems Command, shall ensure all agencies/entities under their sponsorship or direction comply with all provisions of this Order.

5. Administration and Logistics

a. Organizations responsible for formulating policy, writing requirements, developing systems/applications, and validating systems performance must do so per this Order.

b. All developers, owners, and users of information systems have the responsibility to establish and implement adequate operation and IT controls including records management requirements to ensure the proper maintenance and use of

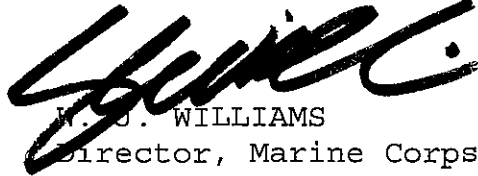
3 Oct 2012

records, regardless of format or medium, to promote accessibility and authorized retention per the approved records schedule.

6. Command and Signal

a. Command. This Order is applicable to the Marine Corps Total Force.

b. Signal. This Order is effective the date signed.



W. S. WILLIAMS
Director, Marine Corps Staff

DISTRIBUTION: PCN 10207711700

**Mission Area Leads, Functional Areas and
Functional Area Managers**

This functional alignment provides a means to categorize, understand and manage Marine Corps current IT systems, applications, and databases. The Marine Corps is a stakeholder within the SECNAV/OPNAV functional areas and shall provide a representative to ensure Marine Corps requirements are captured.

Mission Area Leads

Business Mission Area (BMA)	Marine Corps Business Enterprise Office (MCBEO)
Enterprise Information Environment Mission Area (EIEMA)	Dir C4/DDCIO(MC)
Marine Corps portion of DON Intelligence Mission Area (DON IMA)	Dir Intel
Warfighting Mission Area (WMA)	DC CD&I

DON (SECNAV) Functional Area

Acquisition	CG MCSC
Civilian Personnel	DC M&RA
Legal	SJA to CMC
Financial Management	DC P&R

Navy (OPNAV) Functional Area

Medical	Medical Officer of the Marine Corps
Meteorology, Oceanography, and Geospatial Information and Services	DC AVN

USMC Functional Area

Command & Control	DC CD&I (CDD)
Enterprise Services	Dir C4/DDCIO(MC)
Information Operations	DC PP&O
Intelligence	DIR INTEL
Logistics	DC I&L
Modeling & Simulation	DC CD&I (TECOM)
Personnel Management	DC M&RA
Readiness	DC PP&O
Resources, Requirements & Assessments	DC P&R
Scientific & Technical	DC CD&I (MCWL)
Test & Evaluation	CG MCOTEA
Training & Education	DC CD&I (TECOM)
Weapons Planning & Control	DC CD&I (CDD)

Definitions

1. Analysis. The activity in which portfolio authorities, in collaboration with Components, establish performance goals, identify gaps and opportunities, provide for continuous improvement, and explore functional and technical options as documented in current capabilities and future integrated architectures. The Analysis activity addresses the critical front-end requirements for strategic planning, performance and results management, benchmarking, elimination of unnecessary functions, process improvement, and definition of capabilities and gaps. It creates a directional foundation for the other activities.
2. Application. Any software that uses an existing operating system program to provide the user with a specific capability or function that is independent of other "applications." If it is dependent on other applications, it becomes a system.
3. Authoritative Data Source. A source of data or information that is recognized to be valid or trusted because it is considered to be highly reliable or accurate or is from an official publication or reference.
4. Business Mission Area (BMA). The BMA ensures the right capabilities, resources, and materials are delivered to our warfighters: what they need, where they need it, when they need it, anywhere in the world. In order to cost effectively meet these requirements, DON's current business and financial management and infrastructure processes, systems, and data standards are being transformed to ensure better support to the warfighter and improve accountability to the taxpayer.
5. Commercial-Off-The-Shelf (COTS). Ready-made by commercial vendors and available for sale, lease, or license to the general public, as well as to the Federal Government. COTS software includes desktop and server tools, applications, operating systems, and back office software that is employed in support of DON systems.
6. Control. The activity focused on acquiring the capabilities selected for the portfolio. It consists of acquisition and oversight activities at the portfolio level that complement and supplement traditional single-system, single-platform acquisition and oversight activities.

3 Oct 2012

7. Data. A representation of facts/concepts/or instructions in a formalized manner suitable for communication/interpretation/or processing by humans or by automatic means.

8. Database. A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; the data are stored so that different programs can use them without concern for the data structure or organization.

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

10. DoD Information Technology Portfolio Repository (DITPR) - DON. The DoD single authoritative data source repository for key information and data regarding IT systems, including NSS.

11. DON Application and Database Management System (DADMS). A Web-enabled registry of Navy and Marine Corps systems/applications and their associated data structures. It is the authoritative source for DON IT (including NSS) application and database PFM.

12. Enterprise Architecture (EA). The explicit description and documentation of the current and desired relationships among business and management processes and IT. It describes the "current architecture" and "target architecture" to include the rules and standards and systems life-cycle information to optimize and maintain the environment which the agency wishes to create and maintain by managing its IT portfolio. The EA must also provide a strategy that will enable the agency to support its current state and also act as the roadmap for transition to its target environment. These transition processes will include an agency's capital planning and investment control processes, agency EA planning processes, and agency systems life-cycle methodologies. The EA will define principles and goals and set direction on such issues as the promotion of interoperability, open systems, public access, compliance with Government Paperwork Elimination Act, end-user satisfaction, and IT security. The agency must support the EA with a complete inventory of agency information resources, including personnel,

Enclosure (2)

3 Oct 2012

equipment, and funds devoted to information resources management and IT, at an appropriate level of detail.

13. Enterprise Information Environment (EIE) Mission Area (EIEMA). The EIEMA represents common, integrated information computing and communications environment of the GIG. The EIE is composed of GIG assets that operate as, provide transport for and/or assure local area networks, campus area networks, tactical, operational and strategic networks, metropolitan area networks, and wide area networks. The EIE includes computing infrastructure for the automatic acquisition, storage, manipulation, management, control, and display of data or information, with a primary emphasis on DON enterprise hardware, software operating systems that support the DoD GIG enterprise. The EIE also includes a common set of enterprise services, called "Core Enterprise Services," which provides awareness of, access to, and delivery of information on the GIG.

14. Evaluation. Activity focused on measuring and assessing the outcomes of portfolio investments to determine whether expected benefits were achieved. Primary mechanisms for evaluation are post-implementation reviews. Evaluation results feed back into the other activities of IT PFM to guide all investment decisions and recommendations. Authorities lead the evaluation of outcomes and are primarily responsible for seeing that planned benefits are attained.

15. Functional Area (FA). An FA encompasses the scope (boundaries) of a set of related functions and data for which an OSD Principal Staff Assistant or the Chairman of the Joint Chiefs of Staff (CJCS) has DoD-wide responsibility, authority, and accountability. An FA (e.g., personnel) is composed of one or more functional activities (e.g., recruiting), each of which consists of one or more functional processes (e.g., interviews).

16. Government-Off-The-Shelf (GOTS). Retained and maintained inside the U.S. government (e.g., because it is classified or export controlled).

17. Information Assurance (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.

Enclosure (2)

3 Oct 2012

18. Information Technology (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, including computers, ancillary equipment, software, firmware and similar services and related resources whether performed by in-house, contractor, other intra-agency or intergovernmental agency resources/personnel. Both system and non-system IT resources including base level units (communications, engineering, maintenance, and installation) and management staffs at all levels are included in IT resource reporting.

19. Intelligence Mission Area (IMA). The IMA includes IT investments within the Military Intelligence Program of the National Intelligence Program. The DoD portion of IMA is known as DIMA. DON's portion of DIMA is referred to as DON IMA.

20. Interoperability. Systems, units, and forces shall be able to provide and accept data, information, materiel, and services to and from other systems, units, and forces and shall effectively interoperate with other U.S. Forces and coalition partners. IT and NSS interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchanged information as required for mission accomplishment.

21. IT Investment. The development and sustainment resources needed in support of IT or IT-related initiatives. These resources include, but are not limited to: research, development, test and evaluation appropriations; procurement appropriations; military personnel appropriations; operations and maintenance appropriations; and Defense Working Capital Fund.

22. IT Portfolio. The collection of IT capabilities, resources, and related investments (i.e., networks, devices, databases, systems, and applications) that are required to accomplish a mission-related or administrative outcome. Includes outcome performance measures (mission, functional, or administrative measures) and a documented return on investment.

23. Knowledge Management (KM). The integration of people and processes, enabled by technology, to facilitate the exchange of operationally relevant information and expertise to increase organizational performance.

Enclosure (2)

3 Oct 2012

24. Mission Area. A defined area of responsibility whose functions and processes contribute to accomplishment of the mission.
25. Net-centric. Relating to or representing the attributes of net-centricity. Net-centricity is a robust, globally interconnected network environment (including infrastructure, systems, processes, and people) in which data is shared timely and seamlessly among users, applications, and platforms. Net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles.
26. Portfolio Management (PFM). The management of selected groupings of IT investments using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability.
27. Selection. The activity that identifies the best mix of investments within available resources to meet integrated Enterprise, Mission Area, Sub-portfolio, and Component strategic goals. Portfolio selection decisions are made using integrated architectures, transition plans, technical criteria, and programmatic trade-offs to satisfy performance measures and achieve desired outcomes.
28. System. Any solution that requires a combination of two or more interacting, interdependent, and or interoperable hardware, software, and/or firmware to satisfy a requirement or capability.
29. Warfighting Mission Area (WMA). The WMA provides lifecycle oversight to applicable DoD component and combatant commander (COCOM) IT investments (programs, systems, and initiatives). WMA IT investments support and enhance the CJCS' joint warfighting priorities while supporting actions to create a net-centric distributed force, capable of full spectrum dominance through decision and information superiority. WMA IT investments ensure COCOMs can meet the CJCS' strategic challenges to win the war on terrorism, accelerate transformation, and strengthen joint warfighting through organizational agility, action and decision speed, collaboration, outreach, and professional development.

Enclosure (2)