VOLUME 2B, CHAPTER 18: "INFORMATION TECHNOLOGY (INCLUDING CYBERSPACE OPERATIONS)"

SUMMARY OF MAJOR CHANGES TO

All changes are denoted by blue font.

Substantive revisions are denoted by an * symbol preceding the section, paragraph, table, or figure that includes the revision.

Unless otherwise noted, chapters referenced are contained in this volume.

Hyperlinks are denoted by *bold, italic, blue and underlined font*.

The previous version dated November 2012 is archived.

PARAGRAPH	EXPLANATION OF CHANGE/REVISION	PURPOSE
180102.A	Moved text	Readability
180102.B	Moved/ added text	Readability
180102.C	Added narrative	New information
180102.F	Moved/added text	Readability
180102.G	Changed due date and moved text/reformatted into numbered lists	New Information
180102.H	Added text	Clarification
180102.I	Added text	Readability
180102.K	Moved text/ changed wording/ reformatted into numbered list	Readability
180102.L	Edited words	Grammar/ Readability
180102.L.2	Replaced Exhibit 300 and 53 references; corrected "Logistics"	Readability
180102.M	Replaced Exhibit 300 and 53 references	Readability
180102.N	Added paragraph	Fact of Life
180102.O	Added paragraph	Fact of Life
180103.A	Replaced Exhibit 300 and 53 references	Readability
180103.C	Moved words & added DITIP references	Readability
180103.D	Replaced Exhibit 300 and 53 references	Readability
180103.E	Added "DITIP"	Fact of Life
180103.F	Replaced "bin" for "UII"	Fact of Life
180103.H.1	Added text	Clarification

PARAGRAPH	EXPLANATION OF CHANGE/REVISION	PURPOSE
180103.H.2	Edited words to delete SNAP-DIAP references	SNAP-DIAP eliminated for use
180103.H.3	Added DoD Cyber Team members for CJB publication	Fact of Life
180103.H.4	Added CMF paragraph	Added Program
180103.I	Edited word	Readability
180103.L	Added ICS/PIT/SCADA paragraph	Added program
180104.A	Added table	Readability
180104.I	Added date to JP 3-12	Readability
180104.K	Added NIS TSP 800-82 reference	Fact of Life
180105.V	Added text for Cyberspace Operations definition	Clarity
180105.W	Added CMF definition	Fact of Life
180105.Y	Added Data Center Budget definition	Fact of Life
180105.AC	Added DoDIN definition	Fact of Life
180105.AD	Added DITIP definition	Fact of Life
180105.AE	Updated Development/Modernization	Fact of Life
180105.AX	Added IT Investment	Fact of Life
180105.AY	Added IT Investment	Fact of Life
180105.AZ	Added Information Technology Resources	Fact of Life
180105.BE	Added JIE definition	Fact of Life
180105.BJ	Added NLCC definition	Fact of Life
180105.BY	Added UII definition	Fact of Life
180105.CA	Added WCF definition	Fact of Life
180105.Y-CA	Renumbered paragraphs	Readability
180202.A	Changed “WILL” to “shall”	Readability
180304.A	Edited text	Readability
Various	Changed references to Exhibit 300/300A/300B to updated titles	Clarity
Various	Changed references to Exhibit 53 to updated titles	Clarity
Table of Contents	Updated for edited document	Clarity

Table of Contents

CHAPTER 18

INFORMATION TECHNOLOGY (Including Cyberspace Operations)

1801 GENERAL

180101. Purpose

A. This chapter provides instructions applicable to supporting budgetary material and congressional justification for Information Technology (IT) and Cyberspace Operations investments, as well as discussing requirements for contributions to approved Electronic Government (E-Gov) investments. The Deputy Chief Information Officer for Resources and Analysis (DCIO (R&A)) will issue annual supplemental guidance to these instructions that address detailed and amplifying submission requirements, adjustments since publication of these instructions, and submission due dates.

B. These instructions apply to the Office of the Secretary of Defense (OSD), the Military Departments (including their National Guard and Reserve Components), the Joint Staff, Unified Commands, the Inspector General DoD, the Defense Agencies, the DoD Field Activities, the Joint Service Schools, the Defense Health Program, and the Court of Military Appeals, hereafter referred to as the DoD Components.

C. When contextually appropriate, the terms 'investment' and 'initiative' are interchangeable within this chapter.

180102. Submission Requirements

A. General guidance for submission requirements is presented in Volume 2A, Chapter 1 of the DoD Financial Management Regulation (FMR) and in the OSD Program/Budget guidance memos. This chapter covers specific submission and distribution instructions for the IT Budget and Cyberspace Operations Budget submission. All applicable automated database updates/formats will be submitted for both the OSD Program/Budget Estimates Submission and the Congressional Justification submission referred to in the DOD as the President's Budget (PB) request. The office of the DoD Chief Information Officer (DoD CIO) will distribute information, as appropriate, to Congressional committees, Government Accountability Office (GAO) and Inspector General activities in accordance with Office of Management and Budget (OMB) Circular A-11, section 22 only after the OMB database is updated and OMB has approved the information for release.

B. All DoD Components that program, budget, or execute (obligate) resources to/which support IT and Cyberspace Operations in any fiscal year of the Future Years Defense Program (FYDP) will report IT and Cyberspace Operations data in preparation for the DoD Component's inputs to the OMB Circular A-11 (Section 25.5 and Section 51.18), E-Government reviews, governance documents as required by the OMB Circular A-130, "Management of Federal Information Resources," budget analyses, special data calls, and Congressional displays. The term "Exhibit 300" is also known as the "Capital Investment Report" (CIR) or "IT Business Case" and the terms are used interchangeably throughout this document. However, the product previously called the "Exhibit 300A" is now called the "Major IT Business Case" and the "Exhibit 300B" is now called the "Major IT Business Case Detail". All DOD appropriation accounts and funds including Defense Working Capital Fund (DWCF), Other Funding, and IT & Cyberspace Operations portions of the Military Intelligence Program (MIP) are encompassed unless outlined in paragraph D below. All MIP IT resource submissions shall be coordinated with the OUSD(I)/DUSD(PP&R)/MIP Office.

C. This chapter covers IT and Cyber Operations submissions, including Defense Business Systems (DBS), National Security Systems (NSS), Command & Control (C2), Communications and related programs, Combat Identification, Joint Information Environment (JIE), National Leadership Command Capabilities, Cyberspace Operations, Information Assurance (including Information Systems Security), Cyber Mission Forces, Offensive Cyber Operations, Defensive Cyber Operations, Cyber Intelligence Surveillance and Reconnaissance, Operational Preparation of the Cyberspace Environment, Cyber Threat Detection and Analysis (including Insider Threat), meteorological and navigation systems/programs as well as budgeting for contributions to intergovernmental E-Gov investments.

D. The following resources are exempted from IT reporting:

1. U.S. Army Corps of Engineers Civil Works appropriations.

2. IT acquired by a Federal Contractor incidental to performance of a Federal Contract.

3. Programs, projects, and activities embedded in non-C2/Communications programs or weapon systems or embedded in Service force structure and, therefore, not readily identifiable in the budget. DoD CIO will have final determination on what systems, programs, projects, and activities will be reported.

4. Highly sensitive and special access programs whose resources are specifically exempted from budget reporting by the DoD CIO and other OSD authorities. In general, these resources are reviewed through separate budget processes.

5. National Intelligence Program (NIP) resources. The Office of the Director of National Intelligence staff submits NIP via separate mechanisms.

E. All DoD Components and Enterprise Portfolio Mission Areas must prepare separate executive overviews for the President's Budget and the Congressional Justification Submission. DoD CIO will provide guidance with specific areas of interest that must be addressed within the executive overview.

F. DoD CIO will designate investments required to submit a Major IT Business Case (formerly known as the "Exhibit 300A" (aka EX300A)) and a Major IT Business Case Detail (formerly known as the "Exhibit 300B" (aka EX300B)) to meet OMB Circular A-11, Sections 25.5 and 51.18 requirements. The Capital Asset Plan, Business Case, and the congressional Selected Capital Investment Report (SCIR) are not limited to acquisition or development and modernization programs. A-11, Section 51.18 will direct specific discussions on the broad requirements for reporting Electronic Government, Financial, legacy and sustainment investments.

G. Statement of Compliance Requirement: The IT and Cyber Operations submissions are transmitted electronically, however, both the Component CIO and Comptroller/Chief Financial Officer (CFO) must sign a joint or coordinated transmittal memo, on component letterhead, that states their submissions are

1. Complete;

2. Accurately aligned with their primary budget, the DoD Information Technology Portfolio Registry (DITPR), program and/or acquisition materials; and

3. Consistent with:

a. Subtitle III, title 40 (formerly called the Clinger-Cohen Act), as amended, 10 U.S.C. §2222 (Defense business systems only);

b. OMB Circular A-11 and documented exceptions to the Circular;

c. 10 U.S.C. §11319(b)(1)(B)(ii) provides that the CIO of each covered agency certifies that information technology investments are adequately implementing incremental development, as defined in capital planning guidance issued by OMB;

d. DoD CIO budget guidance memoranda;

e. The Paperwork Reduction Act;

f. Paragraph 180102.D of this chapter;

g. Section 508 of the Rehabilitation Act of 1973, Pub. Law 93-112, as amended (29 U.S.C. § 794d; and

h. Other applicable Acts and requirements.

The statement may be based on the Program Manager's statement of compliance. The statement should also include explanations for investments that do not conform to DoD CIO budget guidance memorandum. DoD Components for which all Information Technology resources are exempt from reporting based on Section ***180102.D*** above must submit a Statement of Compliance addressing the specific reasons for their exemption. This memorandum must be submitted annually to the DoD CIO, Deputy Chief Information Officer (DCIO) (Resources and Analysis) on the Submit/Certify date for the President's Budget request as identified on the Information Technology Budget Schedule.

H. If OMB requires additional governance information to accompany the IT Budget and Cyberspace Operations Budget, DoD CIO will determine how these requirements will be met, and provide direction to the Components. DoD CIO will also provide the Components documented guidance as well as training on any applicable changes to the Department of Defense Information Technology Information Portal (DITIP) and/or Select and Native Programming – Information Technology (SNaP-IT) systems which will be used to gather information requested by OMB.

I. Appointment of qualified project managers for investments listed in the IT Budget and Cyberspace Operations Budget is a matter of high-level interest to the OMB. Components are charged to provide complete Program Manager identification and qualification documentation to comply with Project Manager reporting requirements for Major IT Business Case/Major IT Business Case Detail only.

J. 10 U.S.C §2222 (h) requires that the materials submitted by the Secretary of Defense to the Congress in support of the President's budget include information for each business system program for which funding is requested in the budget. For each defense business system program for which funding is requested in the budget, section 2222(h) states that this information is to:

1. Identify the program;

2. Identify all funds proposed for the program, by appropriation, including funds for current services to operate and maintain the program and funds for business systems modernization, identified by specific appropriation;

3. Identify the pre-certification authority and the senior official designated under the provisions of subsection (f) of section 2222 for the program; and,

4. Describe the approval made by the Defense Business Systems Management Committee under the provisions of 10 U.S.C. § 186 for the program.

K. Information Technology investments, reporting for the first time, with funding greater than or equal to $1M (all appropriations) within the DoD FYDP are required to submit a memorandum from the component CIO (with component DCMO for DBS), on Component letterhead, to the DoD CIO, DCIO (Resources and Analysis). This memorandum must minimally indicate:

1. The investment's Unique Investment Identifier (UII)

2. Title,

3. Acronym,

4. Description,

5. If the investment is a DBS,

6. BY justification or funding approach,

7. Current acquisition milestones,

8. Dates for planned entry to future milestones,

9. Current Life Cycle Cost Estimate (LCCE) or FYDP estimate if a LCCE is not yet available,

10. Listing of other DoD participating Components,

11. All associated DITPR Identification (ID) numbers,

12. Responsible Mission Area or equivalent portfolio manager,

13. DoD Segment, and

14. Whether the investment is a financial management or financial feeder system.

New investments will be addressed in a CIR or SCIR, as applicable. “New” investments are “new starts” for purposes of this regulation. “New” investments do not arise from the breaking up of a larger investment into separately managed investments, nor is an investment “new” because of discovery that it had not been reported previously. If a component projects that a new information technology investment will exceed a Major Automated Information System (MAIS) statutory threshold (per 10 U.S.C. Chapter 144A), the component will ensure that the initiative is budgeted in a unique Program Element and not shared by other activities.

L. 10 U.S.C §2445b requires that the Secretary of Defense submit, to the Congress, annual reports on all MAIS acquisition programs, and any major information technology investment products or services that are expected to exceed a MAIS threshold but are not considered to be a MAIS program because a formal acquisition decision has not yet been made with respect to such investment (a.k.a Unbaselined MAIS) or designated a pre-MAIS. This annual report, known as the MAIS Annual Report (MAR), is also a budget exhibit. MARs are to be consistent with the latest President’s Budget Submission.

1. All MAIS, Unbaselined MAIS, MDAP IT Programs, and Pre-MDAP IT Programs will be reported in SNaP-IT as single investments aligned to the Official MAIS and MDAP Lists maintained in the Defense Acquisition Management Information Retrieval (DAMIR) Portal.

2. Components shall ensure that the MAR information is consistent with the most recently submitted President’s Budget. Components must use the same program description in the MAR, IT-1, and Major IT Business Case and Major IT Business Case Detail.

The program description should be precisely worded to consider the Congressional staff audience. In addition, Components shall notify the Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) as soon as the Component anticipates that the program is within 10 percent of an ACAT I or IA program dollar threshold, as required by DoDI 5000.02.

M. Components with investments deemed "Major" (***180105.BH***) are required to provide updates to the Major IT Business Case Detail, via SNaP-IT, that will be made available to the Federal Information Technology Dashboard (ITDB). Updates include changes to Major IT Business Case Detail baselines, planned start/end dates, actual start/end dates, and planned/actual costs. Additional guidance for this process is promulgated in the DoD CIO's annual guidance (see ***180103.A***).

N. Components MUST provide Data Center Budget information for all Data Centers reported in the DoD Federal Data Center Consolidation Initiative (FDCCI) inventory currently maintained in the Data Center Inventory Management (DCIM) (which replaced the Characterization and Dependency Analysis Tool (CADAT)). Data Center budgets will be provided by Development, Modernization, and Enhancement (DME) and Operation and Maintenance (O&M) costs and are maintained in the DITIP Data Center Budget model under "Data Center".

O. Components must identify which investments are resourced through a DWCF's capital program, as well as whether such investment either is an IT product or IT service (vice an investment in a non-IT product or service). The SNaP-IT DWCF IT budget module for IT Working Capital Fund requirements located on the Nonsecure Internet Protocol (IP) Router Network (NIPRNet or "NIPR") will forecast all planned revenue for the Investment to include any classified investment amounts residing in the Secret Internet Protocol Router Network (SIPRNet or "SIPR"). With regard to Working Capital Fund, the data entry requirements and responsibilities are dependent on the role of the organization entering the data. The two roles are "owner" (WCF Owner) or "resource user" (WCF Participant). Refer to OSD guidance for greater details.

180103. Preparation of Material

A. This section covers material reporting requirements for IT resources submitted to the DoD CIO. The DoD CIO will provide an augmenting guidance letter annually by early August of the reporting year. The guidance will include changes in submission requirements to meet A-11 (Section 25.5 and 51.18), E-Government, and Congressional requirements (SCIRs), FY2003 DoD Authorization Act Section 351 requirements, Component Overviews, and Section 332 reporting; special areas of emphasis; and a listing of the investments that require a Major IT Business Case/Major IT Business Case Detail.

B. All IT resources must be managed in accordance with appropriation guidance and applicable expense and investment criteria.

C. All IT resources will be reported within investments. With the exception of Defense business systems (see ***180103.G.2***), MAIS (see ***180102.L.1***), Approved Shared

Services (see ***180103.I***), and programs, projects, and activities exempted by section ***180102.D.4***, investments can be systems, programs, projects, organizations, activities or grouping of systems with related functionality. All references to "Approved Shared Services" should now state "Approved Defense Enterprise IT Services (DEITS). Each Component will manage its classified and unclassified investments through the respective DITIP. Investments are registered with key categories of data required to meet internal and external reporting requirements. To register a new investment or amend/update existing investment data, DoD Components access DITIP's online investment registration capability. A Unique Investment Identifier (UII) is associated with each investment. The current and archived lists of investments are maintained on the DITIP web site. Additional guidance for the registration process, is promulgated in the DoD CIO's annual guidance (see ***180103.A***).

The Department of Defense Information Technology Investment Portal (DITIP) provides a centralized location for IT investment portfolio data, is the authoritative data source for DoD IT Header information, and aligns IT systems information in the Defense IT Portfolio Registry (DITPR) with budget information in the SNaP-IT. DITIP provides for the entry and maintenance of common DITPR and SNaP-IT data elements, provides a mechanism to identify Data Center budget resource estimates and supports the DCMO defense business system (DBS) certification. DITIP is the system of record for the four National Defense Authorization Act (NDAA) Defense Business System data elements (i.e., Business Enterprise Architecture (BEA) Code, BEA Version, Business Process Re-engineering (BPR) Code and Category Critical Capability (CATBC Code).

Components are responsible for verifying investment data entered in DITIP is consistent with that data entered into DITPR. At a minimum each DITPR line item must be aligned against an active SNaP-IT UII.

D. All investments requiring a Major IT Business Case/Major IT Business Case Detail will be identified within the annual IT Budget and Cyberspace Operations Budget guidance (see ***180103.A***). Regardless of actual investment amount, all funding for MAIS and pre-MAIS programs as defined in 10 U.S.C §2245a will be reported in the IT exhibit as major (exceptions to this rule will be annotated in the IT Budget and Cyberspace Operations Budget Guidance). Components that serve as the executive or principal funding agent (aka "Owner") for investments must report all sections of the Major IT Business Case and Major IT Business Case Detail.

E. Investments with multiple participating DoD Components are joint investments. All information submitted for a joint investment is the responsibility of the investment owner registered in DITIP/SNaP-IT. The owner shall coordinate investment data with each participating DOD Component of that joint investment.

F. Group of Systems. With the exception of Defense business systems (see ***180103.G***), MAIS (see ***180102.L.1***), and DEITS (see ***180103.I***), investments can be groupings of systems with related functionality if all the systems are within the same Mission Area, segment, managed under the same construct, and financed under the same resource construct (program/project/organization). All systems grouped into an IT Budget Investment must report that investment's UII in the appropriate DITPR system record.

G. Defense Business Systems (DBS)

1. In order to satisfy requirements of 10 U.S.C. §2222, for certification and approval of investments involving "defense business systems" as "covered defense business system programs," as well as for budget information in the materials that the Secretary of Defense submits to the Congress under 10 U.S.C. §2222(h), investments in defense business systems must be reported individually within the Information Technology (IT) Budget.

2. All defense business systems must be included within the IT Budget at the system level, not as system of systems, group of systems, or bundle of systems (i.e., Defense Business System = Investment).

3. The definition of a DBS is provided in section ***180105.Z***. All systems reported in the DITPR as a DBS, or with the primary mission areas designation of "Business", MUST be maintained as their own SNaP-IT Investment.

H. Cyberspace Operations

1. DOD categorizes Cyberspace Operations as a major reportable category of the DoD Information Network (DoDIN) (formerly known as the Global Information Grid (GIG) IT/ Defense Information Infrastructure (DII)). Strictly for OMB taxonomy and SNaP-IT purposes, there are three components to Cyberspace Operations: Cybersecurity (also known as Information Assurance), Cyberspace Operations, and Research and Development. Cybersecurity is more defensive in nature, whereas Cyberspace Operations is more offensive. Definitions are provided in Joint Publication 3-12. Research and Development efforts that support DoD Cyberspace Operations focuses on the incorporation and fusion of advanced technology with capabilities for defensive and offensive tactics, techniques, practices, and procedures in the cyberspace domain.

2. Components with Cyberspace Operations investments will report its resources through the SNaP-IT System. All Cyberspace Operations resources will be reported within cyberspace operations investments as prescribed by DoD CIO. Justification narratives to support the preparation of the DoD Cyberspace Operations Congressional Justification Book (CJB) will be input directly into SNaP-IT.

3. DoD CIO DCIO Resources & Analysis (DCIO R&A), in coordination with DCIO Cybersecurity and the offices of CAPE, USD(C), USD(I) and USD(AT&L) and components as identified in 180102.(B) will prepare a single DoD Cyberspace Operations CJB containing materials supporting DoD's overall Cyberspace Operations efforts. This information is collected simultaneously with the IT Budget utilizing SNaP-IT. Components must complete the SNaP-IT submission for all investments identified either in the "GIG Group" as Information Assurance Activities (IAA) or in the Segment using "610-000".

4. The Cyber Mission Forces were established in March 2013 and activated in January 2014. The Cyber Mission Forces have three main aspects: 1) Cyber National Mission Teams to help defend the nation against a strategic cyber attack on US interests

including our critical infrastructure and key resources (CIKR); 2) Cyber Combat Mission Teams aligned with regional and functional Combatant Commanders to support their objectives; and 3) Cyber Protection Teams to help defend DoD information environment and the military cyber terrain. These cyber mission teams are the U.S. military's first joint tactical command dedicated to cyberspace operations. They primarily support the Combatant Commands. In order to efficiently account for planned, programmed, and budgeted financial requirements, organizations are required to use the unique taxonomies and Program Elements that SNaP-IT established for the Cyber National Mission Forces. OSD classified guidance and training will provide further details on managing UIIs with appropriate Program Elements and the OMB taxonomies.

I. Defense Enterprise IT Services (DEITS) (Formerly known as Approved Shared Services)

The DoD CIO Executive Board may occasionally authorize a DoD Approved Shared Service. In those cases, an Authorized Shared Service must be reported in a single SNaP-IT investment. The DCIO (Resources and Analysis) will maintain a listing of Authorized Shared Service and provide that listing within the DoD CIO's annual IT Budget and Cyberspace Operations Budget guidance (see ***180103.A***).

J. Industrial Control Systems (ICS)/ Platform Information Technology (PIT)/ Supervisory Control and Data Acquisition (SCADA)

As stated in NIST Special Publication 800-82, "ICS are typically used in industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods.) SCADA systems are generally used to control dispersed assets using centralized data acquisition and supervisory control.…These control systems are vital to the operation of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems." These systems, while not generally considered a typical Information System, are just as vulnerable to interception, modification, interruption and fabrication that threaten typical Information Technology Systems. Likewise, the defensive measures taken to protect ICS/PIT/SCADA systems are similar to the cybersecurity measures currently taken to protect IT systems: Firewalls, Intrusion Detection Systems, strong passwords, and encryption to name a few. Therefore, the documented planning, programming and budgeting of the costs of researching, procuring, operating and maintaining these defensive mechanisms used to protect ICS/PIT/SCADA from these vulnerability exploitations should begin in the FY17 President's Budget using SNaP-IT. PIT CS purchased as part of a weapons systems or some other turn-key non-IT solution (i.e., as part of an HVAC system) would not be reported in the IT/Cyber Budget. In summary, if the turn-key solution is IT then the ICS/PIT/SCADA systems would be reported within the turn-key investments IT/Cyber budget. If the PIT CS is being purchased on its own or upgraded to address cyber security shortfalls, it would be reported in the IT/cyber budget. Lastly there is no need register PIT CS as a separate IT investment -- it can be a part of a larger investment.

180104. References

A. DoD FMR, Volume 2A, Chapter 1 provides general funding and appropriation policies, including expense and investment criteria (Section 010201) and Budgeting for Information Technology and Automated Information Systems guidance (Section 010212), as well as general preparation instructions and distribution requirements. The table below highlights FMR references to the applicable appropriation.

Reference	Appropriation
Volume 2A, Chapter 3	Operation and Maintenance
Volume 2B, Chapter 4	Procurement
Volume 2B, Chapter 5	RDT&E
Volume 2B Chapter 6	Military Construction
Volume 2B Chapter 9	Defense Working Capital Fund (DWCF)

Volume 2B, Chapter 16 discusses requirements for NIP and MIP justification materials. Additional Cyberspace Operations justification guidance is provided above in (***180103.H***) and via an annual guidance letter.

B. DoD Directive 5000.01, "Defense Acquisition," DoD Instruction 5000.02, "Operation of the Defense Acquisition System," and the Defense Acquisition Guidebook discuss acquisition and program management requirements for preparation of acquisition program Capital Asset Plan and Business Cases. DTM 11-003 – Reliability Analysis, Planning, Tracking, and Reporting and DTM 09-027 – Implementation of the Weapon Systems Acquisition Reform Act of 2009 provide further clarification to DoDD 5000.01.

C. Office of Management and Budget (OMB) Circular No. A-11, "Preparation and Submission of Budget Estimates," Section 51.18, "Budgeting for the acquisition of capital assets," and Section 25.5, "What do I include in the budget request?" provide the general Federal reporting requirements for IT resources.

D. The Paperwork Reduction Act of 1995 and the Public Law 104-106 (Clinger-Cohen Act of 1996) contain supporting definitions regarding IT.

E. OMB Circular A-130, "Management of Federal Information Resources" provides guidance on governance requirements including the Documented Capital Planning and Investment Control (CPIC) process, Agency Enterprise Architecture and the Information Resource Management (IRM) Plan.

F. DoD Directive 8115.01, "Information Technology Portfolio Management" and DoD Instruction 8115.02, "Information Technology Portfolio Management Implementation," provides guidance and define responsibilities for DoD Mission Areas.

G. DoD Directive 7045.20, "Capability Portfolio Management," establishes policy and assigns responsibilities for the use of capability portfolio management.

H. DoD Directive 5205.12, "Military Intelligence Program (MIP)," Establishes policy and assigns responsibilities for the MIP in accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (a)) to provide visibility into Defense Intelligence resource data and capabilities and to create a means for effectively assessing Defense Intelligence capabilities.

I. Joint Publication 3-13, Information Operations, dated November 27, 2012.

J. Joint Publications 3-12, Cyberspace Operations, dated February 5, 2013.

K. National Institute of Standards and Technology Special Publication 800-82, June 2011.

L. DoD Directive 8000.01, Management of the Department of Defense Information Enterprise, dated February 10, 2009.

M. DoD Instruction 8500.01, Cybersecurity, dated March 14, 2014.

180105. Definitions

A. Acquisition Management Segment (510-000). IT supporting the activities necessary to provide (non-commodity) goods/services for DoD operations.

B. Battlespace Awareness-Environment Segment (710-000). IT supporting the ability to collect, analyze, predict and exploit meteorological, oceanographic and space environmental data.

C. Battlespace Awareness-ISR Segment (700-000). IT supporting the ability to conduct activities to meet the intelligence needs of national and military decision-makers.

D. Battlespace Networks Segment (720-000). IT that extends DoD's "commercial like" IT Infrastructure to meet the unique connectivity and interoperability needs of deployed and mobile warfighting capabilities. Focuses on information transport, computing, enterprise services capabilities that supports the Combined Joint Task Force. NOTE: All investments included in the Battlespace Networks segment should be identified as NSS. If it is not an NSS system then it probably should be aligned with the Information Technology Infrastructure (ITI) segment.

E. Budget Identification Number (BIN). See Unique Investment Identifier.

F. Building Partnerships Segment (790-000). This segment covers the IT supporting the capability for setting conditions for interaction with partner, competitor or adversary leaders, military forces, or relevant populations by developing and presenting information and conducting activities to affect their perceptions, will, behavior, and capabilities.

G. Business Mission Area (BMA). The BMA ensures that the right capabilities, resources, and materiel are reliably 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, the DoD current business and financial management infrastructure - processes, systems, and data standards - are being transformed to ensure better support to the warfighter and improve accountability to the taxpayer. Integration of business transformation for the DoD business enterprise is led by the Deputy Secretary of Defense in his role as the Chief Management Officer (CMO) of the Department, and supported by the Deputy Chief Management Officer (DCMO).

H. Business Services Segment–TBD (599-000). This is a placeholder for those "few" business service related IT investments that do not currently fit into the existing business segments.

I. Business Services Segment Group. This segment includes investments for foundational mechanisms and back-office services used to support the mission of the agency. Segments included in this group are: Financial Management, Acquisition, Human Resources Management, Logistics/Supply Chain Management, and Installation Support.

J. Communications and Computing Infrastructure (C&CI). The C&CI reporting category includes the information processing (computing), transport (communications) and infrastructure management services used in DoD such as voice, data transfer (including electronic commerce and business interfaces), video teleconferencing, and messaging. The C&CI category is subdivided into operational areas and special interest programs.

K. Communications. Communications elements include fixed plant, sustaining base infrastructure in the US and selected overseas locations; long haul transmissions via Defense-owned or leased terrestrial facilities; transmissions via satellite or other radio systems; and mobile, tactical transmission systems.

L. Command and Control (C2). Includes the facilities, systems, and manpower essential to a commander for planning, directing, coordinating and controlling operations of assigned forces. C2 capabilities cover the joint/tactical operations echelon and down to front line tactical elements.

M. Command and Control Segment (730-000). This segment provides the IT that facilitates the exercise of authority and direction over DoD-mission related activities supporting the joint warfighter.

N. Computing Infrastructure. Automated information processing operations reported in the C&CI section generally perform one or more of the following functions: processing associated with agency-approved automated information systems; timesharing services; centralized office automation; records management services; or network management support. Staff associated with these operations includes computer operators, computer system programmers, telecommunications specialists, helpdesk personnel and administrative support personnel.

O. Core Financial System. Is an information system, or system of system, that may perform all financial functions including general ledger management, funds management, payment management, receivable management, and cost management. The core financial system is the system of record that maintains all transactions resulting from financial events (see definition below). It may be integrated through a common database or interfaced electronically to meet defined data and processing requirements. The core financial system is specifically used for collecting, processing, maintaining, transmitting, and reporting data regarding financial events. Other uses include supporting financial planning, budgeting activities, and preparing financial statements. Any data transfers to the core financial system must be: traceable to the transaction source; posted to the core financial system in accordance with applicable guidance from the Federal Accounting Standards Advisory Board (FASAB); and in the data format of the core financial system.

P. Core Mission Services Segment (799-000). Placeholder for those "few" core mission service related IT investments that do not currently fit into the existing core service segments.

Q. Core Mission Services Segment Group. This segment group contains investments that directly support the Department's core missions. Segments included in this group are; Battlespace Awareness – Environment, Battlespace Awareness – Intelligence, Surveillance, and Reconnaissance (ISR), Battlespace Networks, Command and Control, Force Application, Protection, Building Partnerships, Force Management, Force Training, and Health.

R. Cost. A monetary measure of the amount of resources applied to a cost objective. Within the DoD, "costs" are identified following the GAO accounting principles and standards as implemented in this Regulation. The fact that collections for some cost elements are deposited into Miscellaneous Receipts of the Treasury does not make those costs "extraneous." It simply means the Congress has not authorized such amounts to be retained by appropriation accounts. After costs have been identified, following the Comptroller General cost accounting rules, a DoD Component may proceed to eliminate cost elements, or process waivers, in accordance with legal authorities.

S. Current Services (CS). At the Federal level, this is referred to as Steady State (SS) and is synonymous with operations and maintenance. Current Services represents the cost of operations at the current capability and performance level of the application, infrastructure program and/or investment when the budget is submitted. That is, the cost with no changes to the baseline other than fact-of-life reductions, termination or replacement. Current Services include: (1) personnel whose duties relate to the general management and operations of information technology, including certain overhead costs associated with Program Management (PM) offices; (2) maintenance of an existing application, infrastructure program or investment; (3) corrective software maintenance, including all efforts to diagnose and correct actual errors (e.g., processing or performance errors) in a system; (4) maintenance of existing voice and data communications capabilities; (5) replacement of broken IT equipment needed to continue operations at the current service level; (6) Technical Refresh; and (7) all other related costs not identified as Development/Modernization.

T. Cybersecurity. As referenced in DoDI 8500.01 "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

U. Cyberspace**.** A global domain consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

V**.** Cyberspace Operations**.** Employment of cyberspace capabilities for the primary purpose of achieving objectives in or through cyberspace. For the purposes of budget reporting within the OMB taxonomy and SNaP-IT, there are three major components of Cyberspace Operations: Cybersecurity (also known as Information Assurance), Cyberspace Operations, and Research & Development. Refer to paragraphs T and AU for more information. The DoD DCIO (R&A) office will provide further guidance on Cyberspace Operations via classified channels.

W. Cyber Mission Forces. The U.S. military's first joint tactical command with a dedicated mission focused on cyberspace operations and primarily support the Combatant Commands and USCYBERCOM.

X. Data Administration. Program Area of Related Technical Activities. Activities reported in this area include: Data sharing and data standardization. Component data administration programs are defined in the Data Administration Strategic Plans.

Y. Data Center Budget. All Data Centers reported in the DoD FDCCI inventory currently maintained in the DCIM (which replaced the CADAT) must maintain an appropriate budget estimate in DITIP at all times. Each Data Center budget line will include the following information:

1. Resourcing Component,

2. DCIM Unique ID,

3. SNaP-IT Investment UII,

4. Resource Type (DM/CS)

    a. DME - Development, Modernization, and Enhancement, or

    b. CS - Operations and Maintenance (Steady State)

5. Prior Year (PY) through Budget Year plus 4 (BY+4) Resources

Z. Defense Business System (DBS). The term "defense business system" as defined at 10 U.S.C §2222(j)(1) means 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 information technology and information assurance infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management. The term "covered defense business system" as defined at 10 USC §2222(j)(2) means any defense business system program that is expected to have a total cost in excess of $1,000,000 over the current future-years defense program submitted to the Congress under 10 U.S.C §221.

AA. Defensive Cyberspace Operations (DCO). Passive and active operations to preserve the ability to utilize friendly cyberspace capabilities and protect the DoD networks and net-centric capabilities,

AB. Defensive Cybersecurity. The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

AC. Department of Defense Information Network. The DoD Information Network (DoDIN) (formerly called the Global Information Grid (GIG), as defined in DoD Directive 8000.01 as well as JP 3-13), is the globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The DODIN includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. The DODIN consists of information capabilities that enable the access to, exchange, and use of information and services throughout the Department and with non-DoD mission partners. The principal function of the DODIN is to support and enable DoD missions, functions, and operations. The overarching objective of the DODIN vision is to provide the National Command Authority (NCA), warfighters, DoD personnel, Intelligence Community, business, policy-makers, and non-DoD users with information superiority, decision superiority, and full-spectrum dominance.

AD. Department of Defense Information Technology Investment Portal (DITIP). DITIP provides a centralized location for IT investment portfolio data and aligns IT systems information in the Defense IT Portfolio Registry (DITPR) with budget information in the Select and Native Programming Data Input System for IT (SNaP-IT). DITIP provides for the entry and maintenance of common DITPR and SNaP-IT data elements and supports the DCMO defense business system (DBS) certification.

AE. Development/Modernization (Dev/Mod). Also referred to as development/modernization/enhancement. Development, Modernization and Enhancement refers to projects and activities leading to new IT assets/systems, as well as projects and activities that change or modify existing IT assets to substantively improve capability or performance, implement legislative or regulatory requirements, or meet an agency leadership request. DME activity may occur at any time during a program's life cycle. As part of DME, capital costs can include hardware, software development and acquisition costs, commercial off-the-shelf acquisition costs, government labor costs, and contracted labor costs for planning, development, acquisition, system integration, and direct project management and overhead support. Technical Refresh is NOT included in Dev/Mod, but rather in Current Service as discussed previously.

AF. DoD portion of Intelligence Mission Area (DIMA). The DIMA includes IT investments within the Military Intelligence Program and DoD component programs of the National Intelligence Program. The USD(I) has delegated responsibility for managing the DIMA portfolio to the Director, Defense Intelligence Agency, but USD(I) retains final signature authority. The DIMA management will require coordination of issues among portfolios that extend beyond the Department of Defense to the overall Intelligence Community.

AG. Enterprise Information Environment Mission Area (EIEMA). The EIEMA represents the common, integrated information computing and communications environment of the GIG. The Enterprise Information Environment (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 the DoD enterprise hardware, software operating systems, and hardware/software support that enable the GIG enterprise. The EIE also includes a common set of enterprise services, called Core Enterprise Services, which provide awareness of, access to, and delivery of information on the GIG.

AH. Enterprise Services Segment –TBD (699-000). This is a placeholder for those “few” enterprise service related IT investments that do not currently fit into the existing IT Infrastructure; Identity and Information Assurance; or IT Management segments.

AI. Enterprise Services Segment Group. This segment group includes investments for IT services and infrastructure that support core mission and business services. Segments included in this group are; Identity and Information Assurance (IIA), IT Infrastructure, and IT Management.

AJ. Financial Event. Is any activity having financial consequences to the Federal government related to the receipt of appropriations or other financial resources; acquisition of goods or services; payments or collections; recognition of guarantees, benefits to be provided, or other potential liabilities; distribution of grants; or other reportable financial activities.

AK. Financial Management Segment (500-000). The IT supporting the facilitation and implementation of financial management solutions providing timely and accurate decision support data, stronger internal controls, establishing standards for acquiring and implementing FM systems through shared business processes, IT services, and data elements.

AL. Financial Management Systems. Financial Management systems perform the functions necessary to process or support financial management activities. These systems collect, process, maintain, transmit, and/or report data about financial events or supporting financial planning or budgeting activities. These systems may also accumulate or report cost information, support preparation of financial transactions or financial statements or track financial events and provide information significant to the DoD Components financial management.

AM. Force Application Segment (740-000). IT supporting the capability to integrate the use of maneuver and engagement in all environments, to creating the necessary effects for achieving DoD mission objectives.

AN. Force Management Segment (770-000). IT supporting the ability to integrate new and existing human and technical assets from across the Joint Force and its mission partners to make the right capabilities available at the right time/place to support National Security.

AO. Force Training Segment (780-000). IT supporting the ability to enhance the capacity to perform specific functions and tasks in order to improve the individual or collective performance of personnel, units, forces, and staffs.

AP. Global/Functional Area Applications (G/FAA). Also referred to as Global Applications, Global, or Functional Area Applications are associated with all DoD mission areas—C2, Intelligence and combat support, combat service support areas, and the DoD business areas. Selected investments will be categorized as NSS. Global applications rely upon the network, computing and communication management services including information processing, common services, and transport capabilities of the Communications and Computing Infrastructure. Related technical activities provide the architectures, standards, interoperability, and information assurance that these applications require to operate effectively as part of the Defense Information Infrastructure. Although an application/system may serve more than one function, it is generally classified according to the predominate function across the department. Each Functional Application category is subdivided into Functional Areas that equate to principal staff functions and activities.

AQ. Global Information Grid (GIG). This term is now referred to as the DoD Information Network (DODIN) which is described in paragraph ***AB*** above. Until the term “GIG” is removed, replaced or updated in all applicable documentation, this definition will remain in this document for reference purposes. The GIG supports all DoD missions with information technology for National Security Systems, joint operations, Joint Task Forces, Combined Task Force commands, and DoD business operations that offer the most effective and efficient information handling capabilities available, consistent with National Military Strategy, operational requirements and best value enterprise level business practices. The GIG is based on a common, or enterprise level, communications and computing architecture to provide a full range of information services at all major security classifications.

AR. Health (760-000). The Health segment facilitates the implementation of IT systems and services that enable the Department’s capabilities to maintain the health of military personnel, which includes the delivery of healthcare required during wartime.

AS. Human Resource Management Segment (520-000). IT supporting DoD human resource management, personnel and readiness ensuring human resources are recruited, trained, capable, motivated, and ready to support the Department.

AT. Identification Number (IN). Investment numbers are more commonly referred to as the Budget Identification Numbers (BIN). A four or five digit identification number that is assigned to each investment, program and system reported in the IT budget and Cyberspace Operations Budget.

AU. Identity and Information Assurance (IIA) Segment (610-000). IT supporting the DoD's ability to maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation and availability of data and information at rest and in transit. IIA's purpose is to maintain the information and information assets; document threats and vulnerabilities; ensure the trustworthiness of users and interconnecting systems; determine the impact of impairment or destruction to the DoD information system(s) and cyberspace; and manage cost effectiveness.

AV. Information Assurance (IA). With regard to OMB taxonomy and SNaP-IT purposes, when referencing Paragraph ***T***, DOD considers "Information Assurance" synonymously with "Cybersecurity", which is one of three components of Cyberspace Operations, and is a major reportable category of the DoDIN/IT/JIE. The term "Information Assurance" and "Cybersecurity" are used interchangeably throughout this chapter. However, DoDI 8500.01 primarily uses "Cybersecurity" as the most current terminology concerning Information Assurance and as such, future publications will remove "Information Assurance" references. For a historical perspective, IA included all efforts that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Also included were all provisions for restoration of information systems by incorporating protection, detection, and reaction capabilities. As such, IA was broader in scope than information systems security and reflected the realities of assuring timely availability of accurate information and reliable operation of DoD information systems in increasingly inter-networked information environments.

AW. Information System (IS). (Reference section 3502 of title 44 U.S.C.) An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. This includes automated information systems (AIS), enclaves, outsourced IT-based processes and platform IT interconnections. To operate information systems, Components must support related software applications, supporting communications and computing infrastructure and necessary architectures and information security activities.

AX. Information Technology (IT). (Reference section 11101 of title 40 U.S.C. and PL 113-291, Subtitle D –Federal Information Technology Acquisition Reform Act) The term "information technology" is defined as:

1. Services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency; and

2. Services or equipment that are used by an agency if used by the agency directly or if used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.

3. The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources.

4. The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment.

AY. Information Technology (IT) Investment. This term refers to the expenditure of IT resources to address mission delivery and management support. An IT investment may include a project or projects for the development, modernization, enhancement, or maintenance of a single IT asset or group of IT assets with related functionality, and the subsequent operation of those assets in a production environment. All IT investments should have a defined life cycle with start and end dates, with the end date representing the end of the currently estimated useful life of the investment, consistent with the investment's most current alternatives analysis if applicable. When the asset(s) is essentially replaced by a new system or technology, the replacement should be reported as a new, distinct investment, with its own defined life cycle information.

AZ. Information Technology Resources. The term "information technology resources" is defined as:

1. Agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, disposition, and transformation, or other activity related to the lifecycle of information technology;

2. Acquisitions or interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements; but

3. Does not include grants to third parties which establish or support information technology not operated directly by the Federal Government

BA. Information Technology (IT) Portfolio. The DoD IT portfolio consists of investments representing a common collection of capabilities and services. The portfolios are an integral part of the Department's decision making process and are managed with the goal of ensuring efficient and effective delivery of capabilities while maximizing the return on Enterprise investments.

BB. Installation Support Segment (540-000). IT supporting the ability to provide installation assets and services necessary to support the US military forces.

BC. IT Infrastructure Segment (600-000). Commercial-like, common user, information transport, computing and (infrastructure) enterprise services supporting DoD's fixed base users in accomplishing their missions.

BD. IT Management Segment (800-000). Facilitates planning, selection, implementation and assessment of IT investments and programs supporting the broader enterprise. This includes: IT strategic planning, promulgation of policy and direction governing the provisioning of services; establishing and maintaining enterprise architectures and transition strategies; cost analysis, performance measurement and assessment in order to best mitigate risks.

BE. Joint Information Environment. The Joint Information Environment (JIE) is a fundamental shift in the way the Department of Defense (DoD) will consolidate and manage Information Technology (IT) infrastructure, services, and assets in order to realign, restructure, and modernize how the Department's IT networks and systems are constructed, operated, and defended. JIE will consolidate and standardize the design and architecture of the Department's networks. The JIE represents the DoD migration from military service-centric IT infrastructures and capabilities, with their mixture of disparate networks and applications, to enterprise capabilities based on common infrastructure and shared services to support Joint needs. These needs include networks, security services, cyber defenses, data centers, and operation management centers. Consolidation and standardization will result in a single, reliable, resilient, and agile information enterprise for use by the joint forces and mission partners. The vision of JIE is to ensure that DoD military commanders, civilian leadership, warfighters, coalition partners, and other non-DoD mission partners have access to information and data provided in a secure, reliable, and agile DoD-wide information environment. The ultimate beneficiary of JIE is the commander in the field, allowing for innovative integration of information technologies, operations, and cybersecurity at a tempo more appropriate to today's fast-paced operational conditions. The objective is for authorized users to access required information and resources from anywhere, at any time, using any approved device across the JIE, enabling warfighter information sharing and mission operations. Since JIE is not a Program of Record, it should be noted that the Department will utilize existing DoD Component programs, initiatives, technical refresh plans, acquisition processes, and funding to deploy and migrate the existing infrastructure to the JIE standards. OSD guidance and training will provide more details concerning the alignment of UIIs to achieving JIE goals and standards.

BF. Life-Cycle Cost (LCC). LCC represents the total cost to the Government for an IS, weapon system, program and/or investment over its full life. It includes all developmental costs, procurement costs, MILCON costs, operations and support costs, and disposal costs. LCC encompasses direct and indirect initial costs plus any periodic or continuing sustainment costs, and all contract and in-house costs, in all cost categories and all related appropriations/funds. LCC may be broken down to describe the cost of delivering a certain capability or useful segment of an IT investment. LCC normally includes 10 years of sustainment funding following Full Operational Capability (FOC) or Full Deployment for Automated Information Systems. For investments with no known end date and that are beyond FOC, LCC estimate should include 10 years of sustainment.

BG. Logistics/Supply Chain Management Segment (530-000). IT supporting the ability to project and sustain a logistically ready joint force to meet mission objectives.

BH. Major. A system or investment requiring special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property or other resources. Systems or investments that have been categorized as “Major” can include resources that are associated with the planning, acquisition and /or sustainment life cycle phases. Large infrastructure investments (e.g. major purchases of personal computers or local area network improvements) should be considered major investments. Includes programs identified as MAIS (also called ACAT IA) in DoD 5000 series documents.

BI. Military Intelligence Program (MIP). The MIP consists of programs, projects, or activities that support the Secretary of Defense’s intelligence, counterintelligence, and related intelligence responsibilities. This includes those intelligence and counterintelligence programs, projects, or activities that provide capabilities to meet warfighters’ operational and tactical requirements more effectively. The term excludes capabilities associated with a weapons system whose primary mission is not intelligence.

BJ. National Leadership Command Capabilities (NLCC). A capability encompassing the entirety of the DoD command, control, communications, computer, intelligence, surveillance, and reconnaissance systems and services that provides national leadership, regardless of location and environment, with diverse and assured access to integrated, accurate, and timely data, information, intelligence, communications, services, situational awareness, and warnings and indications from which planning and decision-making activities can be initiated, executed, and monitored. OSD guidance and training will provide more details concerning the alignment of UIIs to the NLCC.

BK. National Security Systems (NSS). (Reference section 3542 of title 44 U.S.C.) NSS includes any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, or command and control of military forces. NSS also includes equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions. NSS DOES NOT include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

BL. Obligation. The amount representing orders placed, contracts awarded, services received, and similar transactions during an accounting period that will require payment during the same, or a future, period. Obligations include payments for which obligations previously have not been recorded and adjustments for differences between obligations previously recorded and actual payments to liquidate those obligations. The amount of obligations incurred is segregated into undelivered orders and accrued expenditures - paid or unpaid. For purposes of matching a disbursement to its proper obligation, the term obligation refers to each separate obligation amount identified by a separate line of accounting.

BM. Offensive Cyberspace Operations. JP 3-12 defines Offensive Cyberspace Operations as "Cyberspace operations intended to project power by the application of force in or through cyberspace. However, for SNaP-IT and OMB taxonomy purpose, Offensive Cyberspace Operations are activities that actively gather information, manipulate, disrupt, deny, degrade, or destroy adversary computer information systems, information, or networks through cyberspace.

BN. Office Automation (also referred to as "Desktop Processing"). Facilities that support file servers or desktop computers used for administrative processing (e.g. word processing, spreadsheets, etc.) rather than application processing, should be reported as Office Automation (listed as a separate function).

BO. Operational Preparation of the Environment. Non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations. OPE in cyberspace includes identifying data, software, systems, networks, and facilities to determine vulnerabilities and activities to assure future access or control during anticipated hostilities.

BP. "Other" Category (also referred to as "All Other"). For those "Development/Modernization" and/or "Current Services" costs/obligations as well as investments not designated in the major categories. "Other" category investments are aligned with the applicable GIG/IT/DII Reporting Structure functional/mission area (see Section 180106).

BQ. Program Cost (also referred to as investment cost and total acquisition cost). The total of all expenditures, in all appropriations and funds, directly related to the IS, program, or investment's definition, design, development, and deployment; incurred from the beginning of the "Concept Exploration" phase through deployment at each separate site. For incremental and evolutionary program strategies, program cost includes all funded increments. Program cost is further discussed in DoD 5000 series documents.

BR. Protection Segment (750-000). IT supporting the capability to prevent and/or mitigate adverse effects of attacks on personnel (combatant or non-combatant) and physical assets of the United States, its allies and friends.

BS. Related Technical Activities (RTAs). RTAs service global/functional applications, C&CI and IA. While RTAs do not provide directly functional applications, data processing, or connectivity, they are required to ensure that the infrastructure functions as an integrated whole and meets DoD mission requirements. RTAs include such things as spectrum management, development of architectures, facilitation of interoperability, and technical integration activities. RTAs are considered necessary "overhead" for the DODIN. See Section 180106 for the DODIN Structure Table. The RTA category is subdivided into limited Program Areas.

BT. Segments. A portfolio management concept required by OMB Circular A-11. Segments serve as the basis for organizing IT investments for both budget management and performance management purposes. Three groups of segments have emerged to characterize the way in which their segments enable functional capabilities of the enterprise – and to differentiate the way in which investments are governed; Business Services Segment Group, Core Mission Services Segment Group, and Enterprise Services Segment Group.

BU. Select & Native Programming-Information Technology (SNaP-IT). The electronic system used by the DoD CIO to collect IT Budget and Cyberspace Operations Budget data and generates reports mandated by the OMB and the Congress. SNaP-IT is a database application used to plan, coordinate, edit, publish, and disseminate Information Technology (IT) budget justification books required by the Congress. SNaP-IT generates all forms, summaries, and pages used to complete the publishing of the IT Congressional Justification materials (the IT-1, overviews, Selected Capital Investment Reports required by Section 351) and the OMB submissions, such as the IT Investment Portfolio Summary, the IT Business Case, and monthly updates to the OMB Information Technology Dashboard. SNaP-IT provides users the ability to gain access to critical information needed to monitor and analyze the IT Budget and Cyberspace Operations Budget submitted by the DoD Components.

BV. Special Interest Communications Programs. Special interest communications programs are reported under IT/DII C&CI division. Electronic Commerce/Electronic Data Interchange and Distance Learning Systems are special interest programs that should be reported in this area. The resource category "Other" may not be used with Special Interest Communications.

BW. Steady State (SS). See definition for Current Services.

BX. Technical Activities. This refers to activities that deal with testing, engineering, architectures and inter-operability.

BY. Threat Detection and Analysis. This refers to activities that identify, characterize, examine, and track previously undefined types and sources of cyber threats against data, system, or network vulnerabilities to determine the risks to particular data, systems, networks, or operations.

BZ. Unique Investment Identifier. Previously called a "BIN", the UII is a database index field automatically generated with the DITPR/SNaP-IT interface when registering or creating a new investment.

CA. Warfighting Mission Area (WMA). The WMA provides life cycle oversight to applicable DoD Component and Combatant Commander IT investments (programs, systems, and investments). WMA IT investments support and enhance the Chairman of the Joint Chiefs of Staff's 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 Combatant Commands can meet the Chairman of the Joint Chiefs of Staff's 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.

CB. Working Capital Fund Investment. The DWCF authority at 10 U.S.C. § 2208 allows the DoD to finance inventories of supplies and provide working capital for industrial and commercial-type activities. DWCF activities are dependent on revenue, as are commercial businesses. DWCFs provide a mechanism for the DoD Components to finance those supply and commercial and industrial activities that have been chartered under Volume 11B, Chapter 2, or this Regulation. It enables such DoD Components to absorb risk in planning investment programs for maintenance and supply. The intent was to allow chartered commercial, industrial and supply management activities to make capital investments when needed and recoup the costs through future year pricing structure.

180106. Reporting Structure

IT investments shall be managed by enterprise portfolios divided into Mission Area portfolios which are defined as Warfighting, Business, DoD portion of Intelligence, and Enterprise Information Environment. In addition, all information technology resources will be associated with a single DoD Segment (see section 180105 for definitions), the Federal Enterprise Architecture (FEA) Business Reference Model (BRM), and the OMB approved Segment. Investments are also reported by appropriation details (Appropriation, Budget Activity (BA), Program Element (PE), Budget Line Item (BLI), Investment Stage and Source (Base/Overseas Contingency Operations (OCO)) and by "major" and "other" categories. SNaP-IT records these business rules. Investments that cross more than one functional area, such as C&CI, RTA, or IAA (Cyberspace Operations), may need to be broken down by area and registered in the Master BIN List maintained in SNaP-IT by the DoD CIO. The reporting area will normally be based upon the preponderance of the mission/capability concept.

Segment Architecture and Information Technology/Defense Information Infrastructure (DODIN) Reporting Structure

Segment Category	Segment Code *-000	Segment Title	Sub-segment Title	GIG Group	Mission Area
BS	500	Financial Management		FAA	BMA
BS	510	Acquisition		FAA	BMA
BS	520	Human Resource Management		FAA	BMA
BS	530	Logistics/Supply Chain Management		FAA	BMA
BS	540	Installation Support		FAA	BMA
BS	599	Business Services TBD		FAA	BMA
ES	600	DoD IT Infrastructure	Core Network Infrastructure	CCI	EIEMA
ES	600	DoD IT Infrastructure	DoD Enterprise Services	CCI	EIEMA
ES	600	DoD IT Infrastructure	DoD IT Infrastructure	CCI	EIEMA
ES	600	DoD IT Infrastructure	Non-Core Network Infrastructure	CCI	EIEMA
ES	610	Cyber Information & Identity Assurance (Cyberspace Operations)	Assured Information Sharing (AIS)	IAA	EIEMA
ES	610	Cyber Information & Identity Assurance (Cyberspace Operations)	Computer Network Defense	IAA	EIEMA
ES	610	Cyber Information & Identity Assurance (Cyberspace Operations)	Cryptographic Key Production and Management	IAA	EIEMA
ES	610	Cyber Information & Identity Assurance (Cyberspace Operations)	Cryptographic Systems	IAA	EIEMA
ES	610	Cyber Information & Identity Assurance (Cyberspace Operations)	Cyber Identify /Access Management	IAA	EIEMA
ES	610	Cyber Information & Identity Assurance (Cyberspace Operations)	Defense Industrial Base (DIB) CyberSecurity/ Information Assurance	IAA	EIEMA
ES	610	Cyber Information & Identity Assurance (Cyberspace Operations)	Engineering & Deployment	IAA	EIEMA
ES	610	Cyber Information & Identity Assurance (Cyberspace Operations)	Information Assurance Operational Resiliency	IAA	EIEMA
ES	610	Cyber Information & Identity Assurance (Cyberspace Operations)	Offensive Cyberspace Operations	IAA	EIEMA
ES	610	Cyber Information & Identity Assurance (Cyberspace Operations)	Workforce Development	IAA	EIEMA
ES	699	Enterprise Services TBD		CCI	EIEMA
CMAS	700	Battlespace Awareness-ISR		FAA	DIMA

Segment Category	Segment Code *-000	Segment Title	Sub-segment Title	GIG Group	Mission Area
CMAS	710	Battlespace Awareness-Environment		FAA	WMA
CMAS	720	Battlespace Networks		CCI	EIEMA
CMAS	730	Command & Control		FAA	WMA
CMAS	740	Force Application		FAA	WMA
CMAS	750	Protection		FAA	WMA
CMAS	760	Health		FAA	BMA
CMAS	770	Force Management		FAA	BMA
CMAS	780	Force Training		FAA	WMA
CMAS	790	Building Partnerships		FAA	WMA
CMAS	799	Core Mission TBD		RTA	EIEMA
ES	800	IT Management		RTA	BMA

BS = Business Systems
ES = Enterprise Services
CMAS = Core Mission Area Services

1802 PROGRAM AND BUDGET ESTIMATES SUBMISSION

180201. Purpose

This section provides guidance for preparation and submission of the Information Technology Budget Estimate Submission (BES) to the DoD CIO, and for preliminary updates to OMB resource exhibits in September in preparation for the OMB "draft guidance" and IT Budget and Cyberspace Operations Budget hearings. Resources reported in the IT submission must be consistent with other primary appropriation justification and FYDP submissions**.** DOD CIO (R&A) will annually issue supplemental guidance for other data requirements directed by the DoD CIO, Congress or OMB. Timelines for updates will be provided as information becomes available and will be designated in the program and budget call memorandum. Technical requirements and templates are provided in SNaP-IT.

180202. Submission Requirements

A. The following information is required. Unless modified in a subsequent budget call, Components shall use the formats in DITIP and on the SNaP-IT Web page (***https://snap.pae.osd.mil/snapit/Home.aspx*** or ***https://snap.cape.osd.smil.mil/snapit/***) and provide an automated submission.

1**.** Investment Registration. Add, update, delete, and modify investment data to accurately represent the current environment for the IT investment and the Component using the DITIP/SNaP-IT investment registration. This includes Titles, Descriptions, Type of IT, IT/NSS Classification, DoD Segment and FEA information, and DoD Component participation requirements.

2. IT Investment Resources. Collection of resources by Component; Security Classification; Appropriation/Fund (Treasury Code); Investment Stage; BA/Line Item; OSD PE Code; Funding Source (Base/OCO); PY, CY, BY, BY+1, +2, +3, and +4 for submitting the IT Investment Portfolio Summary (Exhibit 53) as required by the OMB A-11, Section 51.18 and 25.5.

3. IT Business Case (formerly known as the Exhibit 300). Capital Asset Plan and Business Case (IT) for major investments. The IT Business Case (or CIR), is discussed in the OMB's A-11 Section 51.18 and 25.5. DoD Components are required to complete an IT Business Case for those investments identified by the DoD CIO. In addition to the IT investment resources information reported in the IT Investment Portfolio Summary (Section 180202.A.2), IT Business Case programs will report associated Full Time Equivalent (FTE) personnel and the complete Life Cycle Cost (LCC) of the investment.

B. Distribution of the OSD budget estimates material will be available electronically through the SNaP-IT site.

C. Additional reporting requirements will be identified in the call memorandum, as necessary. Additional management and supporting data may be designated by the DoD CIO to support detailed justification requirements. All supporting program documentation not submitted with the budget submission must be made available to the DoD CIO within two business days of its request.

180203. Arrangement of Backup Exhibits

The SNaP-IT will provide an option to assemble information in the sequence shown in Section 180202, as applicable. Components will be able to generate IT Investment Portfolio Summary (Exhibit 53) level data outputs for internal review only.

1803 CONGRESSIONAL JUSTIFICATION/PRESENTATION

180301. Purpose

This section provides guidance on organizing the IT resource justification materials submitted in support of the President's Budget. The Department will submit draft and final consolidated outputs to the OMB in the January timeframe and for the Congress by the date set by the Comptroller, usually in the first week of March.

180302. Justification Book Preparation

Justification information will be taken from the SNaP-IT system, reflecting the OMB requirements for IT Investment Portfolio Summary (Exhibit 53) and IT Business Case (known previously as the Exhibit 300). Special outputs will be designed for select investments and summaries based on Congressional requirements. DoD Component requirements and review of these outputs will be discussed in the final budget call memorandum. Congressional justification materials will be extracted or derived from materials developed for the OMB updates.

180303. Submission Requirements

Submission requirements are as specified in Section ***180202***, except as noted below:

A. IT Overview. Information Technology Investment Portfolio Assessment Overview is an Executive summary of a DoD Component's and the Enterprise Portfolio Mission Area's IT Investments providing high-level justification of the portfolio selections and priorities. Information provided must be consistent with the Component's overall budget justification materials. A Cyberspace Operations section is required and must be consistent with information reported in cyberspace operations justification materials and financial reporting. Format will be provided via the SNaP-IT web page or the DoD CIO budget guidance.

B. SCIR. Add/Update/Modify SCIR data within SNaP-IT for all investments designated by the DoD CIO as major and therefore submitting an IT Business Case.

180304. Input for Summary Information Technology Justification Books

A. General. All exhibit data shall be submitted in automated form and be consolidated in SNaP-IT (https://snap.pae.osd.mil/snapit/Home.aspx or https://snap.pae.osd.smil.mil/snapit). The DoD CIO is responsible for providing the DoD Information Technology summary tables per Congressional direction. SNaP-IT will generate the OMB and Congressional President's Budget reporting packages after the DoD Component IT Overview and IT Business Case documents have been submitted to the DoD CIO, DCIO (Resources & Analysis) and/or posted to the SNaP-IT web page. SNaP-IT will generate correct identification information, a cover page, a table of contents, an overview and appendices; the IT Index, report, annex and appendix and the IT Business Case or Congressional extract reports. These will generate a single, integrated submission in Adobe Acrobat Portable Document Format (pdf) that can be used for internal coordination. To accomplish this requirement, the DoD Components will populate the SNaP-IT to generate their submission. The DoD CIO will maintain (and make available to the DoD Components and OSD staff) the digital IT Budget and Cyberspace Operations Budget database. Other specific guidance for IT Budget and Cyberspace Operations budget materials will be provided as required.

B. Distribution of the final appropriately released justification material will be made electronically and by Compact Disk Read-Only Memory (CD ROM) to the Congress and the OMB. Releasable information will be available through public web site(s). CD ROMs will be provided to the Government Accounting Office (GAO) and the DoD Inspector General.

1. The DoD CIO will provide data to OMB for review.

2. The DoD Components will send their draft submissions through final Security Review in accordance with Comptroller instructions and provide copies of the appropriate release form to the DoD CIO, DCIO (Resources & Analysis), Office of Information Technology Investment, and as an attachment to the President's Budget Request transmittal form, due within 5 working days of final submission.

3. The DoD CIO will consolidate electronic submissions from the DoD Components and the Enterprise Portfolio Mission Areas and prepare integrated and individual portfolio overviews, summary information and graphics. The justification books will be forwarded to the OMB for review and release approval.

4. Once security and the OMB have released the justification books, summary and detail data will be transmitted to the Congress (House Defense Appropriations Subcommittee, Senate Defense Appropriations Subcommittee, House Armed Services Committee, and Senate Armed Services Committee). Any data made available to the Congress will be available on the public web page(s) and via CD ROM distribution made in accordance with the format, table and media guidance (Justification Material Supporting the President's Budget Request) in ***Volume 2A, Chapter 1***.

1804 INFORMATION TECHNOLOGY PROGRAM SUBMISSION FORMATS

180401. Format Location

The required input formats are located on the *SNaP-IT* Web page *https://snap.pae.osd.mil/snapit/Home.aspx* or *https://snap.cape.osd.smil.mil/snapit/*