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 July 2010 is archived.

PARAGRAPH	EXPLANATION OF CHANGE/REVISION	PURPOSE
180102.B	Update A-11 citation	Update
180102.C	Inclusion of Cyberspace Operations reporting	New Requirement
180102.D	Removes the exemption for reporting Non-Appropriated Funds (NAF)	New Requirement
180102.D.3	Clarifies that DoD CIO has final determination on what systems, programs, projects, and activities will be reported.	Update
180102.L.1	Clarify MAIS reporting	Update
180102.M	Clarify EX300s baseline reporting	Update
180103.G	Clarify Defense Business System reporting	Update
180103.I	Changed the section from Information Assurance to Cyberspace Operations to encompass new reporting requirements	Update
180103.J	Added Approved Shared Services	New Requirement
180104.K	Added DoD Directive 5205.12 Military Intelligence Program	Update
180105	Added multiple definitions	Update
180106	Added Segment Architecture structure	Update

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.

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, here after 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. Only after the Office of Management and Budget (OMB) database is updated and OMB has approved the information for release, will the Office of the DoD Chief Information Officer (DoD CIO) further distribute information, as appropriate, to Congressional committees, General Accounting Office (GAO) and IG activities in accordance with OMB Circular A-11, section 22.

B. All DoD Components that have resource obligations supporting IT and Cyberspace Operations in any fiscal year of the Future Year Defense Plan (FYDP), will report IT and Cyberspace Operations data in preparation for the DoD Component's inputs to the OMB Circular A-11 (Section 25.5and 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 Exhibit 300 is also known as the Capital Investment Report (CIR) and the two terms will be used interchangeably throughout this document. 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, Cyberspace Operations, Information Assurance (including Information Systems Security), Offensive Cyber Operations , Defensive Cyber Operations , Operational Preparation of the Environment, Threat Detection and Analysis, 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 an Exhibit 300A (EX300A) and Exhibit 300B (EX300B) to meet OMB Circular A-11, Sections 25.5 and 51.18 requirements. The Capital Asset Plan, Business Case and Selected Capital Investment Report (SCIR), a congressional report, are not limited to acquisition or development and modernization programs. A-11, Section 51.18 will direct you to 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 CIO and the Comptroller/Chief Financial Officer (CFO) of the Component must sign a joint or coordinated transmittal memo, on component letterhead, that states their submissions are complete; accurately aligned with their primary budget, the DoD Information Technology Portfolio Registry (DITPR), program and/or acquisition materials; and are consistent with subtitle III, title 40 (formerly called the Clinger-Cohen Act), 10 U.S.C. §2222 (Defense business systems only), OMB Circular A-11 and documented exceptions to the Circular, DoD CIO budget guidance memorandum, the Paperwork

Reduction Act, Section 180102.D, 29 U.S.C. §794d (Section 508 of the Rehabilitation Action of 1973, Pub. Law No. 93-112, as amended), and 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) by February 14th (or the following business day).

H. If the OMB requires additional governance information to accompany the IT Budget and Cyberspace Operations Budget, the DoD CIO will determine how these requirements will be met, and provide direction to the Components via the DoD CIO Executive Board.

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 Exhibit 300 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. Investments in information technology reporting for the first time with $1M (all appropriations) or more within the DoD FYDP are required to submit a memorandum from the component CIO, on DoD Component letterhead, to the DoD CIO, DCIO (Resources and Analysis). At a minimum, this memorandum must indicate the investments Budget Identification Number (BIN), title, acronym, description, if the investment is a DBS, BY justification, current acquisition milestones, dates for planned entry to future milestones, current Life Cycle Cost Estimate (LCCE) or FYDP estimate if a LCCE is not yet available, listing of other DoD participating Components, all associated DITPR Identification (ID) numbers, responsible Mission Area or equivalent portfolio manager, DoD Segment, and 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 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. "New" investments are "new starts" for purposes of this regulation. 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, not to be 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 is expected to exceed a MAIS threshold but is 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.

1. All MAIS, Unbaselined MAIS, MDAP IT Programs, and Pre-MDAP IT Programs will be reported in Select and Native Programming – Information Technology (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 other budget exhibits, for example the IT-1 and SCIR. It is highly desirable that the MAR, IT-1, and EX300A and EX300B use the same program description. The program description should be thoroughly edited to contemplate the Congressional staff audience. In addition, Components shall notify the Under Secretary of Defense (Acquisition, Technology, and Acquidistion) (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.BB) are required to provide updates to the EX300B, via SNaP-IT, that will be made available to the OMB Federal Information Technology Dashboard (ITDB). Updates include changes to EX300B 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)).

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 on or about July 15th 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 an Exhibit 300.

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.J), and programs, projects, and activities exempted by section 180102.D.4, investments can be systems, programs, projects, organizations, activities or grouping of systems. Each Component will manage its investments through the SNaP-IT web site, located at

https://snap.pae.osd.mil/snapit/Home.aspx or https://snap.pae.osd.smil.mil/snapit for Cyberspace operations and classified programs. 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 SNaP-IT's on-line investment registration capability. A unique Budget Identification Number (BIN) is associated with each investment. The current and archived lists of investments are maintained on the SNaP-IT web site. New and amended investments are validated by various entities (Deputy Chief Information Officer (DCIO), Portfolio Managers, Investment Review Board staff, Mission Area staff, DoD Architects, etc.) prior to approval and activation in SNaP-IT. Additional guidance for this registration process, known as "Open Season", is promulgated in the DoD CIO's annual guidance (see 180103(A)). Components are responsible for ensuring investment data entered in SNaP-IT is consistent with that data entered into DITPR. At a minimum each DITPR line item must be aligned against an active SNaP-IT BIN.

D. All investments required to submit an EX300A & B (CIR and SCIR) will be identified within the annual IT Budget and Cyberspace Operations Budget guidance 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 EX300A & B.

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 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 Approved Shared Services (see 180103.J), investments can be groupings of systems 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 BIN 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.W. All

systems reported in the DITPR as a DBS MUST be maintained as their own SNaP-IT Investment.

H. Financial Management and Financial Feeder Systems

Core Financial Management systems, as defined in 180105.AH, are reported in SNaP-IT and DITPR. Financial feeder systems must report a percentage estimate indicating how much of the investment is financially focused in the Budget Year. These percentages are captured in the SNaP-IT per investment.

I. Cyberspace Operations

1. DoD categorizes Cyberspace Operations, formally known as and limited to Information Assurance (IA), as a major reportable category of the Global Information Grid (GIG) IT/ Defense Information Infrastructure (DII).

2. Components with Cyberspace Operations investments will report its resources through the Select & Native Programming Data Input System Defense-wide Information Assurance Program (SNaP-DIAP) website located at https://paesso.cape.osd.smil.mil/DIAP. All Cyberspace Operations resources will be reported within cyberspace operations investments as prescribed by DoD CIO. Components are responsible for ensuring cyberspace operations resource data entered into SNaP-DIAP is consistent with the data entered into SNaP-IT. Justification narratives to support the preparation of the DoD Cyberspace Operations Congressional Justification Book (CJB) will be input directly into SNaP DIAP.

3. The DoD CIO DCIO Cybersecurity (DCIO CS), will prepare a single DoD Cyberspace Operations CJB containing materials supporting DoD's overall Cyberspace Operations efforts. This information will be collected with the IT Budget and Cyberspace Operations Budget submission utilizing the SNaP-DIAP, a module of SNaP-IT. Components must complete the SNaP-DIAP submission for all investments identified as Information Assurance Activities (IAA's) in the "GIG Group".

J. Approved Shared Services

The DoD CIO Executive Board may from time to time 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)).

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. Volume 2A,

Chapter 3 provides guidance on Operation and Maintenance appropriations, Volume 2B, Chapter 4 addresses requirements for Procurement appropriations, Volume 2B, Chapter 5 addresses RDT&E, Volume 2B, Chapter 6 provides specific policies related to Military Construction appropriations, and Chapter 9 provides specific policies related to the 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.I) 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. Information System is defined in section 3502 of title 44 U.S.C.

H. National Security System is defined in section 3542 of title 44 U.S.C.

I. Information Technology is defined in section 11101 of title 40 U.S.C.

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

K. 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.

L. Joint Publication 3-13, Information Operations, dated 13 February 2006.

M. Joint Publications 3-12, Cyberspace Operations, dated [in draft].

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 Infracture (ITI) segment.

E. Budget Identification Number (BIN). See Identification Number.

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; and (6) all other related costs not identified as Development/Modernization.

T. 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.

U. Cyberspace Operations. Employment of cyberspace capabilities for the primary purpose of achieving objectives in or through cyberspace. For the purposes of budget reporting, DOD CATEGORIZES CYBERSPACE OPERATIONS AS A MAJOR REPORTABLE CATEGORY OF THE GIG/IT/ DEFENSE INFORMATION INFRASTRUCTURE (DII). Information Assurance (IA), Offensive Cyberspace Operations, Defensive Cyberspace Operations, Operational Preparation of the Environment, and Threat Detection and Analysis are subsets of the Cyberspace Operations MAJOR REPORTABLE CATEGORY.

V. 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.

W. 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.

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

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

Z. Development/Modernization (Dev/Mod). Also referred to as development/modernization/enhancement. Any change or modification to an existing Information System (IS), program, and/or investment that results in improved capability or performance of the baseline activity. Improved capability or performance achieved as a by-product of the replacement of broken IT equipment to continue an operation at the current service levels is not categorized as Development/Modernization. Development/Modernization includes: (1) program costs for new applications and infrastructure capabilities that are planned or under development; (2) any change or modification to existing applications and infrastructure capabilities which is intended to result in improved capability or performance of the activity. These changes include (a) all modifications to existing operational software (other than corrective software maintenance); and (b) expansion of existing capabilities to new users; (3) changes mandated by the Congress or the Office of the Secretary of Defense; (4) personnel costs for Project Management.

AA. 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.

AB. 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.

AC. 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.

AD. 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.

AE. 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.

AF. Financial Feeder Systems. Financial Feeder Systems are sometimes also referred to as mixed or secondary financial systems. Financial feeder systems are information systems that support functions with both financial and non-financial aspects, such as logistics, acquisition, and personnel. They provide key information required in financial processes. For a feeder system, all DoD Components must report the percentage of each feeder system that supports financial requirements.

AG 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.

AH. 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.

AI. 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.

AJ. 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.

AK. 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.

AL. 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 its predominate function across the department. Each Functional Application category is subdivided into Functional Areas that equate to principal staff functions and activities.

AM. Global Information Grid (GIG). 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.

AN. 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.

AO. 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.

AP. 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.

AQ. 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. Maintain the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction to the DoD information system(s) and

cyberspace; and cost effectiveness.

AR. Information Assurance (IA). DOD CATEGORIZES IA AS PART OF CYBERSPACE OPERATIONS, A MAJOR REPORTABLE CATEGORY OF THE GIG/IT/ DEFENSE INFORMATION INFRASTRUCTURE (DII). IA includes all efforts that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Also included are all provisions for restoration of information systems by incorporating protection, detection, and reaction capabilities. As such, IA is broader in scope than information systems security and reflects the realities of assuring timely availability of accurate information and reliable operation of DoD information systems in increasingly inter-networked information environments.

AS. Information System (IS). 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.

AT. Information Technology (IT). IT means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes computers, ancillary equipment, IT services, software, firmware and similar services and related resources whether performed by in-house, contractor, other intra-agency or intergovernmental agency resources/personnel.

AU. Information Technology & Information Technology Resources. The Information Technology (IT) Resources that must be reported under this chapter are defined by the OMB Circular A-11 and described by subtitle III of title 40 (formerly called the Clinger-Cohen Act of 1996) and include NSS resources. The term investment within the OMB A-11 is very broad and includes IT resources in all life cycle phases (planning, acquisition or steady state). 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. Additional guidance regarding IT systems will be addressed in the annual IT Budget and Cyberspace Operations Budget and DITPR Guidance memos.

AV. 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.

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

AX. 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.

AY. 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.

AZ. 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.

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

BB. 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.

BC. Mixed System. See Financial Feeder System.

BD. 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.

BE. National Security Systems (NSS). 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).

BF. 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.

BG. Offensive Cyber Operations. Activities that actively gather information, manipulate, disrupt, deny, degrade, or destroy adversary computer information systems, information, or networks through cyberspace.

BH. 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).

BI. 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.

BJ. "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).

BK. 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.

BL. 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.

BM. 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 GIG/DII. See Section 180106 for the GIG/IT/DII Structure Table. The RTA category is subdivided into limited Program Areas.

BN. 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.

BO. 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 Exhibit 53, the Exhibit 300s, 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.

BP. 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.

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

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

BS. 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.

BT. 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.

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 category 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 (IT/DII) Reporting Structure

Segment Category	Segment Code	Segment Title	GIG Group	Mission Area
Business Services	500-000	Financial Management	FAA	BMA
Business Services	510-000	Acquisition	FAA	BMA
Business Services	520-000	Human Resource Management	FAA	BMA
Business Services	530-000	Logistics/Supply Chain Management	FAA	BMA
Business Services	540-000	Installation Support	FAA	BMA
Business Services	599-000	Business Services TBD	FAA	BMA
Enterprise Services	600-000	DoD IT Infrastructure	CCI	EIEMA
Enterprise Services	610-000	Information & Identity Assurance (Cyberspace Operations)	IAA	EIEMA
Enterprise Services	699-000	Enterprise Services TBD	CCI	EIEMA
Core Mission Area Services	700-000	Battlespace Awareness-ISR	FAA	DIMA
Core Mission Area Services	710-000	Battlespace Awareness-Environment	FAA	WMA
Core Mission Area Services	720-000	Battlespace Networks	FAA	EIEMA
Core Mission Area Services	730-000	Command & Control	FAA	WMA
Core Mission Area Services	740-000	Force Application	FAA	WMA
Core Mission Area Services	750-000	Protection	FAA	WMA
Core Mission Area Services	760-000	Health	FAA	BMA
Core Mission Area Services	770-000	Force Management	FAA	BMA
Core Mission Area Services	780-000	Force Training	FAA	WMA
Core Mission Area Services	790-000	Building Partnerships	FAA	WMA
Core Mission Area Services	799-000	Core Mission TBD	RTA	EIEMA
Enterprise Services	800-000	IT Management	RTA	BMA

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**.** Supplemental guidance may be issued 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 WILL use the formats on the SNaP-IT Web page (***https://snap.pae.osd.mil/snapit/Home.aspx*** or ***https://snap.pae.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 SNaP-IT investment registration and 'Open Season' process. 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 Exhibit 53 as required by the OMB A-11, Section 51.18 and 25.5.

3. Exhibit 300. Capital Asset Plan and Business Case (IT) for major investments. The Exhibit 300 (or CIR), is discussed in the OMB's A-11 Section 51.18 and 25.5. DoD Components are required to complete an Exhibit 300 for those investments identified by the DoD CIO. In addition to the IT investment resources information reported in the Exhibit 53 (Section 180202.A.2), Exhibit 300 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 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 Exhibits 53 and 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 Exhibit 300.

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 Exhibit 300 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 Exhibit 300 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 electronically 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 five 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.pae.osd.smil.mil/snapit/*