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

SUMMARY OF MAJOR CHANGES

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 September 2015 is archived.

PARAGRAPH	EXPLANATION OF CHANGE/REVISION	PURPOSE
Throughout the Volume 2B, Chapter 18	Extensive revisions due to evolving and new policies, guidance and statutes, including changing "Cyberspace Operations" to "Cyberspace Activities" and new Segments and definitions.	Addition/ Revision
180102	Re-organized based on guidance for a mandatory "Authoritative Guidance" section	Revision
1802	Re-organized Chapter based on guidance for Definitions to become the 2nd section vice a sub-section within GENERAL	Revision
180104.H	Added paragraph about new Security Operations Centers (SOC) reporting requirements	Addition
180104.I	Added paragraph about new Centrally Managed Enterprise Software License reporting requirements	Addition
180104.J	Added paragraph about new Cloud Environment Investments reporting requirements	Addition
180104.K	Revised paragraph based on new Cyberspace Activities definitions and reporting requirements	Addition
180104.M	Added paragraph about new Artificial Intelligence (AI) reporting requirements	Addition
180105	Updated the "Segment Architecture and Information Technology/Defense Information Infrastructure (DODIN) Reporting Structure" table	Addition

Table of Contents

CHAPTER 18

INFORMATION TECHNOLOGY (INCLUDING CYBERSPACE ACTIVITIES)

1801 GENERAL

180101. Purpose

A. This chapter provides instructions applicable to supporting budgetary material and congressional justification for Information Technology and Cyberspace Activities (IT/CA) investments, as well as discussing requirements for contributions to approved Electronic Government (E-Gov) investments. The Department of Defense (DoD) Chief Information Officer (CIO) Deputy Chief Information Officer for Resources and Analysis (DCIO(R&A)) is responsible for collecting, assembling, and reporting of the Departments IT/CA budget for the purposes of submitting complete and accurate IT/CA justification materials to the Office of Management and Budget (OMB) and the Congress. DoD CIO 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. The budgetary materials developed in accordance with instructions in this and other applicable chapters in Volumes 11A and 11B represent the authoritative DoD IT/CA budget request.

* 180102. Authoritative Guidance

A. DoD Financial Management Regulation (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 following table highlights DoD 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	DWCF

Volume 2B, Chapter 16 discusses requirements for NIP and MIP justification materials. Additional CA justification guidance is provided in ***180104.K*** and via an annual guidance letter.

B. DoD Directive (DoDD) 5000.01, "The Defense Acquisition System," DoD Instruction 5000.02, "Operation of the Defense Acquisition System," and the Defense Acquisition Guidebook discuss acquisition and program management (PM) requirements for preparation of acquisition program Capital Asset Plan and Business Cases.

C. OMB Circular No. A-11, "Preparation, Submission and Execution of the Budget," Section 51.19, "Budgeting for the acquisition of capital assets," and Section 25.5, "What do I include in the budget request to OMB?" 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, as amended) contain supporting definitions regarding IT.

E. OMB Circular A-130, "Managing Information as a Strategic Resource" 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. DoDD 8115.01, "Information Technology Portfolio Management" and DoD Instruction 8115.02, "Information Technology Portfolio Management Implementation," provide guidance and define responsibilities for DoD Mission Areas.

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

H. DoDD 5205.12, "Military Intelligence Program (MIP)," Establishes policy and assigns responsibilities for the MIP in accordance with the authority in 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 20, 2014. This publication provides joint doctrine for the planning, preparation, execution, and assessment of information operations across the range of military operations.

J. Joint Publications 3-12, "Cyberspace Operations," dated June 8, 2018. This publication provides joint doctrine to plan, execute, and assess cyberspace operations.

K. NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security," May 2015. This document provides guidance on how to secure ICS, including SCADA systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements.

L. DoDD 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," dated July 27, 2017. The directive establishes policy and assigns responsibilities for DoD IRM activities of the DoD CIO.

M. DoDI 8500.01, "Cybersecurity," dated March 14, 2014. Provides instruction to establish a DoD cybersecurity program to protect and defend DoD information and IT.

N. DoDI 5000.75, "Business Systems Requirements And Acquisition," January 24, 2020. Implements the statutory requirements of Title 10 USC Section 2222(c) and establishes policy for the use of business capability acquisition (BCAC) cycle for business systems requirements and acquisition.

180103. Submission Requirements

A. General guidance for submission requirements is presented in Volume 2A, Chapter 1 of the DoD FMR and in the OSD Program/Budget guidance memos. This chapter covers specific submission and distribution instructions for the IT/CA 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. DoD CIO will distribute information, as appropriate, to Congressional committees, Government Accountability Office (GAO) and Inspector General activities in accordance with OMB Circular A-11, Section 22 – "Communications With The Congress And The Public And Clearance Requirements" – 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/CA in any fiscal year of the Future Years Defense Program (FYDP), Prior Year (PY) and Current Year (CY) will report IT/CA data in preparation for the DoD Component's inputs to the OMB Circular A-11 (Section 25.5 and Section 51.19), E-Gov reviews, governance documents as required by the OMB Circular A-130, "Managing Information as a Strategic Resource," budget analyses, special data calls, and Congressional displays. 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/CA portions of the Military Intelligence Program (MIP) are encompassed unless outlined in paragraph D. All MIP IT resource submissions shall be coordinated with the Office of the Under Secretary of Defense for Intelligence (OUSD(I))/Directors for Defense Intelligence (Intelligence Strategy, Programs & Resources) (DDI ISP&R/MIP Office)).

C. This chapter covers IT/CA 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, Cybersecurity, Artificial Intelligence (including Information Systems Security and machine learning), 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 systems, control systems, IT/CA associated Research, Development, Testing and Evaluations (RDT&E) and navigation systems/programs as well as budgeting for contributions to intergovernmental E-Gov investments. The IT/CA budget encompasses all DoD appropriation accounts and funds with the exception of nonappropriated funds as defined in DoD FMR Volume 13, Chapter 1.

D. This chapter's IT budget preparation and requirements do not apply to:

1. U.S. Army Corps of Engineers Civil Works (USACE-CW) appropriations.

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

3. Programs, projects, and activities embedded in non-C2 and non-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.

6. A Family of Systems (FoS) or System of Systems (SoS) recorded as such within the Department of Defense Information Technology Portfolio Registry (DITPR), systems within a FoS or SoS are subject to this chapter's requirements.

7. Resources related to systems with an inactive DITPR record (see DITPR Guidance[1], Section 9.4.g, for details).

E. All DoD Components and Enterprise Portfolio Mission Areas must prepare separate executive overviews for 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 (see ***1802.BF***) IT Business Case and Major IT Business Case Details to meet OMB Circular A-11, Sections 25.5 and 51.19 requirements. The Major IT Business Case Detail is designed to coordinate OMB's collection of Agency information for its reports to Congress, as required by the Federal Acquisition Streamlining Act of 1994 (FASA, Title V) and Clinger-Cohen Act of 1996. Currently, IT Business Cases are required for Part 1 (Mission Delivery – Segment 700) and Part 2 (Mission Support Systems – Segment 500) major IT Investments. OMB does not require IT Business Cases for Part 3 (IT Infrastructure, IT Security, and IT Management –Segments 600, 610, and 800). The Business Case and Business Case Detail submissions are not limited to acquisition or development and modernization programs.

G. Statement of Compliance (SoC) Requirement. The IT/CA submissions are transmitted electronically. For that reason, each Component is required to submit a coordinated

[1] DITPR Guidance v1.0 (May 2018), Available on RPB IT Budget Portal at https://dodcio.sp.pentagon.mil/sites/Collaboration/ITBudget/IT%20Budget%20Docs/DITPR%20Guidance%20-%2005302018.pdf

annual transmittal memo known as the "Statement of Compliance" memorandum with their IT/CA submissions, on the Submit/Certify due in accordance with the FY Budget Schedule. The SoC memorandum must be addressed to the DoD CIO and the DoD Chief Management Officer (CMO). Military Departments (MILDEP) must also include their MILDEP CMO as addressee on the SoC memorandum. The Component CIO and CFO, or individual(s) assigned with equivalent responsibilities, must jointly sign the SoC, which states their submissions are complete; accurately aligned with the submitting Component's primary budget, program and acquisition materials; and are consistent with:

- Subtitle III, title 40 (formerly called the Clinger-Cohen Act), as amended, and with 10 U.S.C.§2222 (Defense business systems only);
- OMB Circular A-11 and documented exceptions to the Circular;
- 40 U.S.C. §11319(b)(1)(B)(ii), which 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;
- Federal Information Technology Acquisition Reform Act (FITARA) Title VIII, Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015;
- OMB A-130;
- The Privacy Act;
- DoD CIO IT/CA budget guidance memoranda;
- The Paperwork Reduction Act;
- Section 508 of the Rehabilitation Act of 1973, Pub. Law 93-112, as amended (29 U.S.C. § 794d); and
- Other applicable Acts and requirements.

The statement may be based on the Program Manager's SoC. The statement should also include explanations for investments that do not conform to DoD CIO budget guidance memorandum. DoD Components for which all IT resources are exempt from reporting based on Section ***180103.D*** must still submit a SoC addressing the specific reasons for exemption.

H. If OMB requires additional governance information to accompany the IT/CA 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 (see ***180302***).

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

J. 10 U.S.C §2432 requires that the Secretary of Defense submit, to the Congress, annual reports on all Major Defense Acquisition Programs (MDAP). This annual report,

known as the Select Acquisition Report (SAR) will take the place of the OMB required Major Business Case and Major Business Case Detail exhibits for all MDAP IT programs.

1. All MDAP IT Programs, and Pre-MDAP IT Programs will be reported in DITIP/SNaP-IT (see ***180302***) as single investments aligned to the Official MDAP Lists maintained in the Defense Acquisition Management Information Retrieval (DAMIR) Portal. Some programs may be broken out into increments with different Program Number (PNO) that may be associated with one Investment tied to the main or parent program. In such cases of one Investment to many PNO relationship, the valid one-to-one relationship for budget reporting purposes will continue to be in reference to the parent program.

2. For MDAP IT programs, Components must use the DAMIR program description within DITIP/SNaP-IT. The program description should be precisely worded to consider the Congressional staff audience. In addition, Components shall notify the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) as soon as the Component anticipates that the program is within 10 percent of an Acquisition Categories (ACAT) I or IA program dollar threshold, as required by DoD Instruction (DoDI) 5000.02.

K. Components with investments deemed "Major" (see ***1802.BF***) are required to provide updates to the Major IT Business Case and Major IT Business Case Detail, via SNaP-IT, that will be made available to the OMB 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 ***180104.A***).

L. Components must account for resources to acquire, operate and maintain each data center identified in the Data Center Inventory Management (DCIM) System database. Each Core Data Centers (CDC), Component Enterprise Data Centers (CEDC), and Installation Processing Nodes (IPN) must be reported in a single investment within DITIP/SNaP-IT (see ***180302***). Components may report multiple data centers under one investment for other types of data centers, typically Special Purpose Processing Nodes (SPPN), and are not required to segregate costs. DWCF investments delivering IT Services are not required to have separate investment for each Data Centers.

M. Components must identify which investments are resourced through a DWCF, as well as whether such investment is either an IT product or an IT service (vice an investment in a non-IT product or service). The SNaP-IT DWCF IT budget module for IT Working Capital Fund (WCF) requirements located on the Nonsecure Internet Protocol (IP) Router Network (NIPRNet or "NIPR") will forecast all planned revenue and revenue sources for the Investment to include any classified investment amounts residing in the Secret Internet Protocol Router Network (SIPRNet or "SIPR"). Refer to the annual OSD guidance for greater details.

N. Components are required to provide resourcing, within the timeframe being reported, that represents the total Life Cycle Cost Estimate (LCCE) of the investment.

O. Components must identify and break out resources applied to an investment as a result of directives associated with the annual Program Budget Review (PBR) process (e.g.,

DEPSECDEF Memorandum, Program Budget Decision (PBD), Program Decision Memorandum (PDM)). Refer to the annual OSD IT/CA budget guidance for greater details.

180104. Preparation of Material

A. This section covers material reporting requirements for IT resources submission to the DoD CIO. The DoD CIO will provide augmenting guidance annually, by early August of the reporting year. The guidance will include changes to meet new or updated OMB A-11, OMB E-Gov, Congressional, and OSD submission requirements; 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 (see ***180302.B***). With the exception of DBS (see ***180104.G.2***), Major Automated Information Systems (MAIS) (see ***180104.D***), Approved Shared Services (see ***180104.L***), Data Centers (i.e., CDC, CEDC, IPN) (see ***180103.L***), centrally managed enterprise software license purchases (see ***180104.I and 1802.J***), Cloud projects (***180104.J***), Artificial Intelligence projects (***180104.M***), and Security Operations Centers (SOC) (see ***180104.H and 1802.BW***), investments can be systems, programs, projects, organizations, activities or grouping of systems with *related functionality*. 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 on-line 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 ***180104.A***).

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 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 DoD Chief Management Officer (CMO) DBS certification in accordance with the requirements of Title 10 U.S.C.§2222. DITIP is the system of record for the NDAA DBS data elements (i.e., Business Enterprise Architecture (BEA) Code, BEA Version, Business Process Re-engineering (BPR) Code, Requirements and Plan, Acquisition Strategy, and Auditability Requirement).

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 or valid exception UII. Additional guidance for exception UII's is promulgated in the DoD CIO's annual guidance (see ***180104.A***).

D. All investments requiring a Major IT Business Case/Major IT Business Case Detail will be identified within the annual IT/CA Budget guidance (see ***180104.A***).

Regardless of actual investment amount, all funding for MAIS and pre-MAIS programs (as designated in the authoritative MAIS list maintained by the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) will be reported in the IT exhibit as major. Components that serve as the executive or principal funding agent (a.k.a., "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/validate investment data with each participating DoD Component of that joint investment.

F. Group of Systems. With the exception of DBS (see ***180104.G and 1802.AA***), MAIS, Approved Shared Services (see ***180104.L***), data centers (see ***180103.L***), centrally managed enterprise software license purchases (see ***180104.I and 1802.J***), Cloud projects (***180104.J***), Artificial Intelligence projects (***180104.M***), and Security Operations Centers (SOC) (see ***180104.H and 1802.BW***), 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(i)(1)(A), investments in defense business systems must be reported individually within the IT/CA Budget (see ***180302***).

2. The definition of a DBS is provided in section 180105.AA. All DBS must: (a) be included within the IT/CA Budget at the system level, not as system of systems, group of systems, or bundle of systems (i.e., Defense Business System = Investment); and (b) maintain a one-to-one relationship between DITIP/SNaP-IT and DITPR unless a specific exception is approved by the DoD CIO DCIO(R&A) office. The DoD CMO or military department CMO certifies DBSs prior to obligation of funds in the applicable fiscal year, in accordance with their policies. In cases where the CMO certifies PY or CY resources for a DBS, Components must report the amount certified plus any amount not certified that remain programmed or budgeted for the investment (i.e., Obligations + Commitments + Uncommitted balance) in the appropriate resource line(s) in the budget.

*H. Security Operation Centers (SOC). Components must establish each SOC *(see **1802.BW**)* as an individual investment and report resources accordingly (see ***180302***). All SOC investments and resources will be reported within 'Cyberspace Activities' Segment 610-000 and 'Cybersecurity Network Operation' category of the DoD CA Taxonomy. SOCs may take other names such as Cybersecurity Operation Center (CSOC), Joint Operation Center, Network

and Security Operation Center, Cyberspace Operations and Integration Center (ACOIC).

*I. Centrally Managed Enterprise Software License. Components must develop individual investments for each Centrally Managed Enterprise Software License and report resources in the DoD IT/CA Budget accordingly (see ***180302***). An enterprise license is an organization-wide (i.e., DoD-wide, Component-wide, Subcomponent-wide) software license that provides common usage rights within a defined community of users in the organization and may be customized to the organization's requirement *(see **1802.J**)*. Typically, the defined community of users interface with the Software Publisher/Licensor under a single point of contact (i.e., centrally managed) including for acquisition, payments, inventory reporting, and other contractual actions. Examples of such Enterprise License include: Enterprise License Agreement (ELA), Joint ELA (JELA), Core Enterprise Technology Agreement (CETA), and purchasing agreements such as DoD Enterprise Software Initiative Enterprise Software Agreement (ESI ESA) (e.g. General Services Administration (GSA) IT Schedule 70 Blanket Purchase Agreement (BPA) and National Aeronautics and Atmospheric Administration Solutions for Enterprise Wide Procurement (NASA SEWP) agency catalog), Federal Category Management Leadership Council Best in Class (CMLC BIC) purchasing agreement (e.g. GSA IT Schedule 70 Software SINs and NASA SEWP), and DoD Component-level software purchasing vehicles.

*J. Cloud Environment Investments. Components must develop individual investments for each General Purpose (GP), Fit-for-Purpose (F2P), and Internal cloud Projects and report resources in the DoD IT/CA Budget accordingly (see ***1802.AO***, ***1802.AS***, ***1802.AZ***). Register Cloud investments in DITIP (see ***180302.A***).

*K. Cyberspace Activities (CA).

1. DoD categorizes CA as a major reportable category of the DoD IT/CA budget. *(see **1802.V** and **1802.W**)* There are three components within the CA budget: (1) Cybersecurity (also known as Information Assurance); (2) Cyberspace Operations (CO) - a. Offensive Cyberspace Operations (OCO), b. Defensive Cyberspace Operation (DCO), c. DODIN Operations; and (3) Research and Development of new applications to support the advancement of cybersecurity and cyberspace operations. Definitions are provided each budget year (BY) in OSD CA Implementation Guide.

2. Components with CA investments will report their resources through the SNaP-IT System (see ***180302***). All CA resources will be reported within CA investments as prescribed by DoD CIO. Justification narratives to support the preparation of the DoD CA Congressional Justification Book (CJB) will be input directly into SNaP-IT (see ***180403.B***).

3. Components must align CA resources into specific CA budget lines identified in the DoD CIO DCIO(R&A) CA Appropriation Baseline (CAAB) database to comply with congressional direction for spending funding required for CA.[2] Within the IT/CA Budget submission, all: (a) Research, Development, Test, and Evaluation (RDT&E) CA resources must be programmed, budgeted, justified, and executed from unique RDT&E Projects; (b) Procurement

[2] Fiscal Year 2019 House Appropriation Committee – Defense (HAC-D) report language.

CA resources must be programmed, budgeted, justified, and executed from unique Procurement Line-Items; and O&M CA resources must be programmed, budgeted, justified and executed from unique Operations and Maintenance (O&M) Activity/Sub-Activity Groups (AG/SAG). In order to be included in the Department's CA budget, all projects, line-items, and AG/SAGs reporting CA resources must be approved by the DoD CIO and included within the CAAB. Additional CA guidance will be provided by the DoD CIO DCIO (R&A), as needed.

4. DoD CIO DCIO(R&A), in coordination with DCIO Cybersecurity and the offices of OSD Cost Assessment and Program Evaluation (CAPE), USD(C), OUSD(I), USD(A&S), USD(R&E), Principal Cyber Advisor (PCA), USCC, and Components as identified in ***180101.B*** will prepare a single DoD CA CJB containing materials supporting DoD's overall CA efforts. This information is collected simultaneously with the IT Budget utilizing SNaP-IT. Components must complete the SNaP-IT CA CJB submission for all investments identified in the 'Cyberspace Activities' Segment 610-000.

5. The Cyber Mission Forces were established in March 2013 and activated in January 2014. The Cyber Mission Forces have three main aspects: (a) Cyber National Mission Teams to help defend the nation against a strategic cyber-attack on U.S. interests including our critical infrastructure and key resources (CIKR); (b) Cyber Combat Mission Teams aligned with regional and functional Combatant Commanders to support their objectives; and (c) 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 forces dedicated to CA. 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 (PEs) that SNaP-IT established for manning, training, and equipping of the Cyber Mission Forces. The PEs established for CMFs allow the Department to represent CMFs as a virtual Major Force Program (MFP) for reporting to Congress. OSD classified guidance and training will provide further details on managing UIIs with appropriate PEs and the OMB taxonomies.

L. 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 (see ***180302***). The DoD CIO DCIO(R&A) will maintain a listing of Approved Shared Services and provide that listing within the DoD CIO's annual IT/CA Budget guidance (see ***180101.A***).

*M. Artificial Intelligence (AI). Components must develop individual investments for each AI Project, register, tag as 'Artificial Intelligence', and report resources in the DoD IT/CA Budget accordingly (see ***180302***). All AI investments that are stand-alone AI programs or projects and are not the sub-component of a specific end-item's software will be reported within the 'Artificial Intelligence' Segment 400-000 (see ***1802.B***). All AI investments that are a sub-component of a specific end-item's software that enhances the capabilities of the end-item through AI technologies (e.g., an AI application that is a part of an operational or business system) will be reported in the Segment appropriate for that end-item.

N. Industrial Control Systems (ICS)/Platform Information Technology (PIT)/Supervisory Control and Data Acquisition (SCADA). As stated in National Institute of Standards and Technology (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 IT 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 (Converged Systems) used to protect ICS/PIT/SCADA from these vulnerability exploitations must be captured in the IT/CA budget using SNaP-IT (see ***1802.N, 1802.O and 1802.BR***). PIT Control Systems (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/CA 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/CA budget. If the CS/PIT is being purchased on its own or upgraded to address cyber security shortfalls, it would be reported in the IT/CA budget. Lastly there is no need to register each PIT/CS as a separate IT investment -- it can be a part of a larger investment (see ***180302***). However, each resource owner, at a minimum, is responsible for creating at least one single CS/PIT investment for Converged Systems. Components are required to use the unique taxonomies established for CS/PIT within the 'Cyberspace Activities' Segment 610-000. OSD classified guidance and training will provide further details on managing CS/PIT UIIs with appropriate taxonomies.

180105. Reporting Structure

IT/CA 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[3]. In addition, all IT/CA resources will be associated with a single DoD Segment and DoD Sub-Segment (where applicable) (see section 180105 for definitions), the Federal Enterprise Architecture (FEA) Business Reference Model (BRM), and DoD Segment taxonomy. IT/CA investments are also reported by appropriation details (Appropriation, Budget Activity (BA), Program Element (PE), Budget Line Item (BLI), Investment Stage and Funding Source (Base/Overseas Contingency Operations (OCO)), and by "major" and "other" categories. CA investments must further be assigned the DoD & Federal Cyberspace Activities Taxonomy. SNaP-IT records these business rules. Investments that cross more than one functional area, including Cyberspace Activities, may need to be broken down by area and registered in the Master UII List maintained in DITIP/SNaP-IT by the DoD CIO. The

[3] Information Technology Portfolio Management (DoDD 8115.01) and Information Technology Portfolio Management Implementation (DoDI 8115.02)

reporting area will normally be based upon the preponderance of the mission/capability concept. The DoD CIO DCIO(R&A) will annually issue supplemental guidance for other data requirements directed by the DoD CIO, Congress, or OMB.

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

Segment Code	Segment Title	Sub Segment Code	Sub Segment Title	Mission Area
400-000	Artificial Intelligence (AI)	400	Artificial Intelligence (AI)	WMA
500-000	Financial Management	500	Financial Management	BMA
510-000	Acquisition	510	Acquisition	BMA
520-000	Human Resources Management	520	Human Resources Management	BMA
530-000	Logistics and Supply Chain Management	530	Logistics and Supply Chain Management	BMA
540-000	Real Property Management (EI&E)	540	Real Property Management (EI&E)	BMA
550-000	Planning and Budgeting	550	Planning and Budgeting	BMA
560-000	Training and Readiness	560	Training and Readiness	BMA
570-000	Security Cooperation	570	Security Cooperation	BMA
580-000	Defense Security Enterprise	580	Defense Security Enterprise	BMA
599-000	Other Business Services	599	Other	BMA
600-000	DoD IT Infrastructure	010	Core Network Infrastructure	EIEMA
600-000	DoD IT Infrastructure	020	Non-Core Network Infrastructure	EIEMA
600-000	DoD IT Infrastructure	030	DoD Enterprise Services	EIEMA
610-000	Cyberspace Activities	TBD	TBD	EIEMA
620-000	Centrally Managed Enterprise Software License	620	Centrally Managed Enterprise Software License	EIEMA
700-000	Battlespace Awareness-ISR	700	Battlespace Awareness-ISR	DIMA
710-000	Battlespace Awareness-Environment	710	Battlespace Awareness-Environment	WMA
720-000	Battlespace Networks	720	Battlespace Networks	WMA
730-000	Command & Control	730	Command & Control	WMA
740-000	Force Application	740	Force Application	WMA
750-000	Protection	750	Protection	WMA
760-000	Defense Health	760	Defense Health	BMA
770-000	Force Management	770	Force Management	WMA
780-000	Force Training	780	Force Training	WMA
790-000	Building Partnerships	790	Building Partnerships	WMA
799-000	Core Mission	799	Core Mission	WMA
800-000	IT Management	800	IT Management	EIEMA

*1802 DEFINITIONS

The definitions in this section provide relevant information for the chapter including, segment descriptions, technical capabilities and IT/CA Budget component terms.

A. Acquisition Segment (510-000). IT supporting the activities necessary to provide goods/services for DoD operations, including during the stages of conceptualization, initiation, design, development, test, contracting, production, deployment, modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in, or in support of, military missions. This does not include logistics support, which should be reported within the 'Logistics and Supply Chain Management' Segment (530-000).

B. Artificial Intelligence (AI) Segment (400-000). AI refers to the ability of machines to perform tasks that normally require human intelligence – recognizing patterns, learning from experience, drawing conclusions, making predictions, taking actions, and more – whether digitally or as the smart software behind autonomous physical systems. This segment includes any investments for AI programs or stand-along AI projects. This segment also includes AI supporting activities for creating a common foundation of shared data, reusable tools, frameworks and standards, and edge services, through decentralized development and experimentation such as research, longer-term technology creation, and innovative concepts. Do not include AI resources embedded within end-item software system/application investments; report AI embedded within applications as application costs within the appropriate application Investment.

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

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

E. 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 aligned with the Battlespace Networks segment should be identified as NSS. If it is not an NSS system, then it probably should be aligned with the IT Infrastructure segment (600-000).

F. Budget Identification Number (BIN). See definition for Unique Investment Identifier (UII) (see ***180104.C and 1802.CF)***.

G. 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.

H. 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 CMO of the Department.

I. Business Services Segment Group. This segment includes investments for foundational mechanisms and back-office services used to support the mission of the agency, which encompasses all the segments under the BMA. Segments included in this group are: Financial Management, Acquisition, Human Resources Management, Logistics and Supply Chain Management, Real Property Management (EI&E), Planning and Budgeting, Training and Readiness, Security Cooperation, Defense Security Enterprise, and Defense Health. NOTE: there could be a few defense business services related to IT investments that do not currently fit within the Other business service segments (see ***1802.H***).

J. Centrally Managed Enterprise Software License Segment (620-000). An organization-wide (i.e., DoD-wide, Component-wide, Subcomponent-wide) software license that provides common usage rights within a defined community of users in the organization and may be customized to the organization's requirement. Typically, the defined community of users interface with the Software Publisher/Licensor under a single point of contact (i.e., centrally managed) including for acquisition, payments, inventory reporting, and other contractual actions. Examples include: ELA, JELA, CETA, and purchasing agreements such as DoD ESI ESA (e.g. GSA IT Schedule 70 BPA and NASA SEWP agency catalog), Federal CMLC BIC purchasing agreement (e.g. GSA IT Schedule 70 Software SINs and NASA SEWP), and DoD Component-level software purchasing vehicles.

K. Communications. Communications elements include fixed plant, sustaining base infrastructure in the U.S. 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. Control System. A system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include supervisory control and data acquisition (SCADA), distributed control system (DCS), programmable logic controllers

(PLCs) and other types of industrial measurement and control systems. Examples: Utility monitoring and control systems, building control systems, microgrid control systems.

O. Converged System. A system of systems that includes a combination of traditional IT, control systems, and/or platform information technology.

P. 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. 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.

Q. 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.

R. 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.

S. 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.

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 within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

V. Cyberspace Activities (CA). Employment of cyberspace capabilities for the primary purpose of achieving objectives in or through cyberspace. For the purposes of budget reporting within the SNaP-IT, there are three major components of CA: Cybersecurity, Cyberspace Operations, and Research & Development. Refer to definitions in paragraphs ***180104.K*** and ***1802.W***. The DoD CIO DCIO(R&A) office will provide further guidance on CA budget reporting via classified channels.

W. Cyberspace Activities (CA) Segment (610-000). IT supporting the DoD's ability to maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation and availability; the information and information assets; the documentation of 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 (see ***180104.K***). For the purposes of budget reporting within SNaP-IT, there are three major components of CA: Cybersecurity, Cyberspace Operations, and Research & Development (see ***1802.V***).

X. Cyber Mission Forces (CMF). The U.S. military's first joint tactical command with a dedicated mission focused on Cyberspace Activities and primarily support the Combatant Commands and U.S. Cyber Command (USCYBERCOM). The CMF consists of three elements: (1) the Cyber Protection Force (CPF), (2) Cyber National Mission Forces (CNMF), and (3) Cyber Combat Mission Force (CCMF). Further definition is available in Joint Staff Publication (JP 3-12). For IT/CA budget purposes, the CMF budget represents a virtual Major Force Program and consists of the resource to man, train and equip the CMF.

Y. 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.

Z. Data Center Budget. All Data Centers reported in the DoD Data Center Optimization Initiative (DCOI)[4] inventory currently maintained in the DCIM System must maintain an appropriate budget estimate in DITIP at all times. Components must develop individual investments Core Data Center (CDC), Component Enterprise Data Centers (CEDC), and Installation Processing Nodes (IPN) data centers and report resources in the DoD IT/CA Budget accordingly. Working Capital Funds (WCF) Investments delivering IT Services are not required to have a separate Investment per data center. (see ***180103.L***).

AA. Defense Business System (DBS). The term "defense business system" as defined in10 U.S.C §2222(i)(1)(A) means an information system operated by, for, or on behalf of the DoD, including: financial systems, financial data feeder systems, contracting systems, logistics systems, planning and budgeting systems, installations management systems, and human resource management systems. The term does not include NSS, or an information system used exclusively by and within the defense commissary system or the exchange systems or other instrumentality of the DoD conducted for the morale, welfare, and recreation of members of the armed forces using nonappropriated funds (see 10 U.S.C §2222(i)(1)(B)). The term "covered defense business

[4] OMB M-16-19, Data Center Optimization Initiative (DCOI), Aug 1, 2016 (https://datacenters.cio.gov/policy/m-16-19/)

system" as defined at 10 USC §2222(i)(2) means any defense business system that is expected to have a total amount of budget authority in excess of $50,000,000 over the period of the current future-years defense program submitted to the Congress under 10 U.S.C §221.

AB. Defense Health Segment (760-000). 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. The Defense Health Program provides for worldwide medical and dental services (including delivery of TRICARE benefits) to active forces and other eligible beneficiaries, veterinary services, occupational and industrial health care, specialized services for the training of medical personnel, and medical command headquarters.

AC. Defense Security Enterprise Segment (580-000). IT supporting the activities necessary to provide the organizations, infrastructure, and measures (to include policies, processes, procedures, and products) in place to safeguard DoD personnel, information, operations, resources, technologies, and facilities against harm, loss, or hostile acts and influences, in accordance with DoDD 5200.43. This includes any IT that supports Industrial Security Control systems and the National Security Investigation System. This does not include systems/applications that support CA, which doesn't belong within this business function or the 'Business Mission Area' domain.

AD. Defensive Cyberspace Operations (DCO). Missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. Also called DCO.

AE. Department of Defense Information Network (DODIN). DODIN (as defined in DoDD 8000.01 as well as the Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms)," is the set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and NSS. The DODIN includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and NSS. 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 D0DIN 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.

AF. Department of Defense Information Technology Portfolio Registry (DITPR). DITPR is the enterprise service composed of a centralized consolidated inventory of IT systems. DITPR provides a comprehensive inventory of mission critical and mission essential DoD information systems as required in 10 U.S.C. 2223(a)(5) and DoDD 5144.02. DITPR supports IT portfolio management (PfM) in accordance with the Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource" and DoD enterprise architecture management under 44 U. S. C. 3601. DITPR is used to support portfolio management of the Defense Business Systems (DBS), Information Enterprise Mission Area (EIEMA), Warfighter Mission Area (WMA), and DoD Portion of the Intelligence Mission Area (DIMA).

AG. 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 DITPR with budget information in the SNaP-IT. DITIP provides for the entry and maintenance of common DITPR and SNaP-IT data elements and supports the CMO DBS certification.

AH. Development, Modernization, and Enhancement (DME). DME 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 O&S (see ***1802.BM***).

AI. 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 OUSD(I) has delegated responsibility for managing the DIMA portfolio to the Director, Defense Intelligence Agency, but OUSD(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.

AJ. Enterprise Information Environment Mission Area (EIEMA). The EIEMA represents the common, integrated information computing and communications environment. The Enterprise Information Environment (EIE) is composed of 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. The EIE also includes a common set of enterprise services, called Core Enterprise Services, which provide awareness of, access to, and delivery of information.

AK. 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; CA, IT Infrastructure, and IT Management.

AL. 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.

AM. Financial Management (FM) Segment (500-000). 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. This includes IT systems/applications that support the following core financial capabilities: fund the force, banking and disbursing, pay support, accounting support, cost management, financial operations, and management of financial internal controls. This does not include Planning and Budgeting systems/applications, which should be reported within the 'Planning and Budgeting' Segment (550-000).

AN. Financial Management Systems. FM 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.

AO. Fit-for-Purpose (F2P) Cloud. A cloud environment that meets highly specialized mission requirements that cannot easily be met through a General Purpose Cloud solution and is suitable for scaling to adopt new DoD customers at the enterprise level. Determination criteria include utility for mission, ease of management (including provisioning and reporting), and contract terms.

AP. 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.

AQ. 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.

AR. 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.

AS. General Purpose Cloud. Infrastructure and Platform as a Service (IaaS/PaaS) offerings that meet the majority of the DoD's cloud computing needs across all Components of the enterprise organization.

AT. Human Resources Management Segment (520-000). IT supporting DoD human resource management, personnel and readiness ensuring human resources are recruited, capable, motivated, and ready to support the Department. Human Resources Management is the strategic and operational management of activities related to the performance of the human resources in an organization with functions that include: employee and labor/management relations, compensation and benefits, equal opportunity employment compliance, staffing, and human resource development. This does not include training systems/applications, which should be reported within the 'Training and Readiness' business function.

AU. 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, and necessary architectures and information security activities.

AV. 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" with respect to an executive agency 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.

a. with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage,

analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use-- (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product;

b. 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 support services), and related resources; but

c. does not include any equipment acquired by a federal contractor incidental to a federal contract."

AW. Information Technology/Cyberspace Activities (IT/CA) Investment. The IT/CA budget is collected and reported by IT/CA Investments. Each IT/CA Investment is assigned a Unique Investment Identifier (UII). An IT/CA 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/CA 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.

AX. Information Technology (IT) 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 IT;

2. Acquisitions or interagency agreements that include IT 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 IT not operated directly by the Federal Government.

AY. 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.

AZ. Internal Cloud. Specific F2P solutions for systems and applications that need to operate in a private, on-premises cloud environment due to security or operational reasons.

BA. IT Infrastructure Segment (600-000). DoD IT Infrastructure represents the common, integrated information computing and communications environment of the DODIN and its 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. DoD IT infrastructure includes four major categories: Core Network Infrastructure; DoD Enterprise Services; Security (i.e., all defensive CA as which gets reported under 'Cyberspace Activities' Segment 610-000); Non-Core Network Infrastructure.

BB. 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.

BC. Joint Information Environment (JIE). JIE is a fundamental shift in the way the DoD will consolidate and manage 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.

BD. 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, Military Construction (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.

BE. Logistics and Supply Chain Management Segment (530-000). IT supporting the ability to project and sustain a logistically ready joint force to meet mission objectives and activities, including technical and management activities conducted to ensure supportability, and resources to sustain the system in the field. This includes IT systems/applications that support ordering, shipping, and tracking of materiel.

BF. 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.

BG. 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. MIP resourcing used for IT or Cyberspace Activities (CA) must be included within Components'' IT/CA budget submission.

BH. 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.

BI. National Security Systems (NSS). (Reference section 3552 of title 44 U.S.C.) NSS means any information system (including any telecommunications system) used or operated by an agency contractor of any agency or other organization on behalf of an agency: (1) the function, operation, or use of which- involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or (2) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. 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).

BJ. 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.

BK. Offensive Cyberspace Operations. Joint Publication 3-12 defines Offensive Cyberspace Operations as "Mission intended to project power in and through Cyberspace.".

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

BM. Operation and Sustainment (O&S) Costs. Operation Costs refers to the expenses required to operate and maintain an IT asset that is operating in a production environment. At the Federal level, is also Sustainment, O&S is also referred to as Steady State (SS). O&S costs 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. O&S costs 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) business operations and commercial service; (7) Technical Refresh; and (8) all other related costs not identified as Development/Modernization (Dev/Mod).

BN. Operational Preparation of the Environment (OPE). 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.

BO. "Other" Category (also referred to as "All Other"). For those DME or O&S costs/obligations as well as investments not designated in the major categories. "Other" category investments are aligned with the applicable IT Reporting Structure functional/mission area (see Section ***180105***).

BP. Other Business Services Segment (599-000). This segment is applicable only in very limited cases, for those "few" defense business service related IT investments that do not currently fit within the other business segments. Business systems/applications that would fall within this segment involve or provide inherently managerial functions or provide business functions or capabilities such as case/correspondence/workflow/records management/collaboration, or other staff functions.

BQ. Planning and Budgeting Segment (550-000). IT supporting the facilitation of Defense planning and budgeting functions, in accordance with the DoD Planning, Programming, and Budgeting Execution (PPBE) process (DoDD 7045.14), including: (1) developing a set of actions that have been thought of as a way to do or achieve Defense strategic goals, including a comprehensive financial plan encompassing the totality of receipts and outlays (expenditures); and (2) developing a plan of operations for a fiscal period in terms of estimated costs, obligations, and expenditures; source of funds for financing, including anticipated reimbursements and other resources; and history and workload data for the projected Defense program and activities.

BR. Platform Information Technology (PIT). Computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special-purpose systems. PIT does not include general purpose systems. Examples: HVAC systems or electric vehicle fueling systems.

BS. 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.

BT. 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 U.S, its allies and friends.

BU. Real Property Management Segment (540-000). IT supporting the ability to provide and maintain installation real property assets necessary to support U.S. military forces in a cost effective, safe, sustainable, and environmentally sound manner. This includes the missions to: Improve DoD's use of Installation and Operational Energy in order to enhance military capability, reduce risk, and mitigate cost; Protect DoD mission capabilities from incompatible development from utility-scale energy projects, and other encroachment threats; Protect human health and the environment in an uninterrupted and cost effective manner to include systems acquisition, while ensuring the success of the Defense world-wide mission; Function as

an independently appropriated DoD Headquarter Activity with unique capability to assist states and local governments impacted by base closures and realignments, expansions of military installations, or DoD decisions to cancel or reduce defense acquisition programs, as well as maintain a Compatible Land Use program. This does not include installation security access, which should be reported within the 'Defense Security Enterprise' business function.

BV. Security Cooperation Segment (570-000). IT supporting the facilitation of Security Cooperation activities, in accordance with DoDD 5132.03, undertaken by the DoD to encourage and enable international partners to work with the U.S. to achieve strategic objectives. Security Cooperation activities include all DoD interactions with foreign defense and security establishments, including all DoD-administered security assistance programs, that: build defense and security relationships that promote specific U.S. security interests, including all international armaments cooperation activities and security assistance activities; develop allied and friendly military capabilities for self-defense and multinational operations; and provide U.S. forces with peacetime and contingency access to host nations. This also includes any IT systems/applications that support Foreign Military Sales.

BW. Security Operation Center (SOC). OMB Circular A-11 defines as, "a SOC defends an organization against unauthorized activity within computer networks, including, at a minimum, detecting, monitoring, and analyzing suspicious activity as well as leading the response to malicious activity, contributing to restoration activities, and providing a structure for users to report suspected cybersecurity events. A SOC would generally be composed of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents."

BX. 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.

BY. Select & Native Programming-Information Technology (SNaP-IT). The electronic system used by the DoD CIO to collect IT/CA 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 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 and the OMB submissions, such as the IT Investment Portfolio Summary, the IT Business Case, and monthly updates to the OMB ITDB. SNaP-IT provides users the ability to gain access to critical information needed to monitor and analyze the IT/CA Budget submitted by the DoD Components. SNaP-IT is the authoritative application used by the DoD to report and justify the IT/CA budget resources.

BZ. Special Interest Communications Programs. 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.

CA. Steady State (SS). See definition for Operation & Sustainment (see ***1802.BM***).

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

CC. Technology Refresh. Technology refreshment, as defined in FMR Volume 2A, Chapter 1, Section 010201.D.3.c, is the intentional, incremental insertion of newer technology to improve reliability, improve maintainability, reduce cost, and/or add minor performance enhancement, typically in conjunction with depot or field level maintenance. The insertion of such technology into end items as part of maintenance is funded by the operation and maintenance appropriations. However, technology refreshment that significantly changes the performance envelope of the end item is considered a modification and, therefore, an investment.

CD. 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.

CE. Training and Readiness Segment (560-000). IT supporting the training and readiness of DoD employees performing routine administrative and business functions such as Acquisition, FM (PPBE, accounting and payroll), Human Resources (hire-to-retire and personnel management), Defense Health, logistics, and installation management. Training is the level of learning required to adequately perform the responsibilities designated to the function and accomplish the mission assigned to the system. Training and readiness systems and processes are those involved with teaching needed skills or keeping track of this training. This segment does not include the force mission training and combat readiness. IT supporting force mission training and readiness should be reported within Warfighting Mission Area (WMA)-Force Support.

CF. Unique Investment Identifier (UII). Previously called a "Budget Identification Number (BIN)", the UII is a database index field automatically generated with the DITIP/SNaP-IT interface when registering or creating a new investment.

CG. 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.

CH. Working Capital Fund (WCF) Investment. The Defense WCF (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.

1803 PROGRAM AND BUDGET ESTIMATES SUBMISSION

180301. Purpose

This section provides guidance for preparation and submission of the IT/CA 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/CA Budget hearings. Resources reported in the IT/CA submission must be consistent with other primary appropriation justification and FYDP submissions. DoD CIO DCIO(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 DITIP/SNaP-IT.

180302. Submission Requirements

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 (NIPRNet ***https://snap.cape.osd.mil/snapit/*** or SIPRNet ***https://snap.cape.osd.smil.mil/snapit/***) to provide an automated submission. The OSD budget estimates material will be available electronically through the SNaP-IT site. Additional reporting requirements will be identified in the DoD CIO, DCIO for Resources and Analysis 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.

A. Investment Registration. Add, modify, retire, and un-retire investment and associated data to accurately represent the current environment for the IT investment and the Component using the DITIP investment registration (NIPRNet ***https://snap.cape.osd.mil/ITPortal/*** or SIPRNet https://snap.cape.osd.smil.mil/ITPortal/). This includes Titles, Descriptions, Type of IT, IT/NSS Classification, DoD Segment and FEA information, investment ownership and participation, and other investment unique information.

B. 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 as required by the OMB A-11, Section 51.19 and 25.5. In addition, resources are reported in the Technology Business Management (TBM) framework by TBM Tower and Cost Pool.

C. IT Business Case. Capital Asset Plan and Business Case (IT) for major investments. The IT Business Case, is in accordance with the requirements outlined in OMB A-11 Section 51.19 and 25.5. DoD Components are required to complete an IT Business Case for those investments determined as Major by the DoD CIO. In addition to the IT investment resources information reported in the IT Investment Portfolio Summary (Section ***180302.B***), IT Business Case investments will report associated Full Time Equivalent (FTE) personnel, and provide the Milesone Decision Authority (MDA) approved program schedule and Life Cycle Cost Estimate (LCCE) of the investment.

180303. Arrangement of Backup Exhibits

The SNaP-IT will provide an option to assemble information in the sequence shown in Section 180302, as applicable. Components will be able to generate IT Investment Portfolio Summary level data outputs for internal review only.

1804 CONGRESSIONAL JUSTIFICATION/PRESENTATION

180401. Purpose

This section provides guidance on organizing the IT/CA resource justification materials submitted in support of the PB. 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.

180402. Justification Book Preparation

Justification information will be taken from the SNaP-IT system, reflecting the OMB requirements for IT Investment Portfolio Summary and IT Business Case. 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.

180403. Submission Requirements

Submission requirements are as specified in Section 180302, except the following:

A. IT Overview. IT 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. CA section is required and must be consistent with information reported in CA justification materials and financial reporting. Format will be provided via the SNaP-IT web page or the DoD CIO budget guidance.

B. Congressional Justification Book. Beginning with the FY 2021 President's Budget submission, Congress directed the Department to submit the IT/CA Budget no later than 5 days after OMB releases the overall President's Budget submission to Congress. The unclassified Congressional justification submission will consist of the following elements: a) Overview of the IT Budget, b) IT-1 Spreadsheet, c) Cloud Report, and d) Standard Investment Reports. The classified Congressional justification submission will consist of the following elements: a) Overview of the IT/CA Budget; b) IT-1 Spreadsheet; c) Cloud Report; d) CJB for Cyberspace Activities (including O&M OP-5/OP-32 docs, RDT&E R-2A docs, and Procurement P-1 docs); and e) Standard Investment Reports. The due date for these materials is based on OUSD(C) timelines governing the development and submission of the overall Department budget. The submission of the Cyberspace Activities Congressional Justification Book's supporting documents must be uploaded to DITIP. Due date details will be provided in the annual IT/CA Budget Schedule.

180404. Input for Summary Information Technology Justification Books

A. All exhibit data shall be submitted in automated form and be consolidated in SNaP-IT (NIPRNet ***https://snap.cape.osd.mil/snapit/*** or SIPRNet ***https://snap.cape.osd.smil.mil/snapit/***). The DoD CIO is responsible for providing the DoD IT summary tables per Congressional direction. SNaP-IT will generate the OMB and Congressional PB reporting packages after the DoD Component IT Overview and IT Business Case documents have been submitted to the DoD CIO, DCIO(R&A) 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/CA Budget database. Other specific guidance for IT/CA Budget materials will be provided as required.

B. 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 unclassified data made available to the Congress will be available on the public web page(s) in accordance with the format, table and media guidance (Justification Material Supporting the PB Request) in Volume 2A, Chapter 1.

1805 INFORMATION TECHNOLOGY PROGRAM SUBMISSION FORMATS

180501. Format Location

The required input formats are located on the SNaP-IT web page NIPRNet ***https://snap.cape.osd.mil/snapit/*** or SIPRNet ***https://snap.cape.osd.smil.mil/snapit/***