Table of Contents

Summary of Changes

The following revises references to background information and updates citations to reflect current guidance, including OMB Budget Guidance for FY 2018.

Large structural changes:

- Updated text to be consistent with modified A-11 Section 55.
- Updated IT spending categories to now be limited to four categories.
- Added requirement for Agency Budget Account Summary.
- Clarified Agency regular update requirements; reiterated that there is no monthly update requirement, while emphasizing that Agencies are to update the dashboard within 30 days from a change in status of various elements of the Investment.
- Added Standard IT Investments.

Updates to Agency IT Investment Portfolio Summary requirements:

- Question 3: Added Investment Category for USSM-designated shared services.
- Question 10: Added Investment Category for National Security Systems.
- Question 32, 34, & 36: Changed FTE percent to FTE cost for PY, CY, and BY.
- Question 40, 41, and 42: Removed Functional/Business Sponsor phone number, extension, and e-mail.
- Question 42a, 42b, and 42c: Replaced with new Question 39 containing updated language to reflect decisions on usage of cloud computing.
- Questions 52, 53, and 54: Added new questions for Agency IT security spending costs.
- Question 55: Added new question to collect Agency End of Life spending costs.

Updates to Agency Provisioned IT Service Summary requirements:

- Removed requirement for Agencies to report costs for Provisioned IT services by cloud computing service models.

Updates to Agency Data Center Spending Summary requirements:

- Removed all Telecom and End User fields, along with the Data Center Migration and Other Service Contracts fields.

Significant Updates to Major IT Business Case requirements:

- Updated guidance to specify that Investment artifact submission will be only upon request.
- Question 6: Updated language to remove description of corrective actions.
- Updated Section D to include a second table for planned acquisitions.
- Added Section E for Systems Inventory (Administrative Services and Support Systems only).
- Added Section F for Cost & Capabilities (IT Security and Compliance Standard Investment).

Significant Updates to Major IT Business Case Detail requirements:

- Provided framework for agile-based project activities.
- Updated language to include description of operational analysis last date and results.
- Consolidated Project and Operational Risk reporting into single table for Investment-level Risk reporting.

Other:

- Updated Appendix A. Legal Regulatory Authorities to reference US Code, where applicable.
- Updated Appendix B. Added USSM Officially Designated Shared Services with OMB E-Gov and Line of Business Initiatives.
- Added Appendix C. Added a list of common IT Budget – Capital Planning definitions.
- Added Appendix D: Added IT Security definitions.

1. How does the IT Budget – Capital Planning Guidance relate to A-11 Section 55?

Office of Management and Budget (OMB) Circular A-11 Section 55 provides the policy and requirements associated with IT budget, information technology (IT) Investment, and IT portfolio management, whereas the IT Budget – Capital Planning Guidance includes technical requirements and more details related to the requirements. The required information allows the Agency and OMB to review and evaluate each Agency's IT spending and to compare IT spending across the Federal Government.

2. How do I submit annual, quarterly, and regular updates of IT budget and management information, and when is it due?

The Agency's IT Budget and Management information is composed of two parts, the Agency IT Portfolio Summary and the Major IT Business Case. The following tables display the composite budget organization:

Agency IT Portfolio Summary	
Agency IT Investment Portfolio Summary	Part 1: IT Investments for Mission Delivery
	Part 2: IT Investments for Administrative Services and Support Systems
	Part 3: IT Investments for IT Infrastructure, IT Security, and IT Management
	Part 4: IT Investments for Grants and Other Transferred Funding to Non-Federal Organizations for IT
Agency Provisioned IT Services Spending Summary	
Agency Data Center Spending Summary	
Agency Budget Accounts Summary	

Cybersecurity is a top priority for the Administration, and Agencies are now required to report on their standard Investments for IT Security and Compliance at the level that it is managed and executed. In the spirit and support of Federal Information Security Management Act (FISMA) and Federal Information Technology Acquisition Reform Act (FITARA), every organization managing a security program must now report a business case to provide visibility of costs and outcomes of its cybersecurity activities. The intent is not a single, consolidated business case for IT Security and Compliance across the Agency, rather individual Investments reflecting the point at which they are managed. For the security Investments that currently exist and have been reporting Major IT Business Cases, Agencies can individually appeal section exceptions to their respective OMB desk officer in writing (via e-mail).

Major IT Business Case		All Investments (Except Security)	Existing Security Investment*	New Security Investment*
IT Business Case Overview	Section A: General Information	X	X	
	Section B: Investment Details	X	X	
	Section C: Life Cycle Costs	X	X	
	Section D: Acquisition/Contract Strategy	X	X	X
	Section E: Systems Inventory (Administrative Services and Support Systems only)	(Only applicable to Administrative Services and Support Systems Investments)		
	Section F: IT Security Costs & Capabilities (for IT Security and Compliance Investments only)		X	X
	Section A: General Overview	X	X	

Major IT Business Case		All Investments (Except Security)	Existing Security Investment*	New Security Investment*
Major IT Business Case Details	Section B: Project Plan and Execution Data	X	X	
	Section C: Operational Data	X	X	

Note: Major IT Business Case sections marked with an "X" are required submissions for that type of Investment.

Note: For cyber programs run by a central office or entity, the budget data needs to be included in an Agency Office of the Chief Information Officer (OCIO) Security and Compliance Investment as a contribution in order to capture the full cost of security at the enterprise level. Component-level cyber programs should also complete a security business case for services they manage and/or operate and NOT for the funds transferred to the enterprise level to pay for enterprise-wide solutions.

Agencies shall submit materials for the annual, quarterly, and regular updates of IT budget and management information on the following schedule:

2.1 Annual Reporting:
Due to the nature of the transition year, the timing for the IT Budget Submissions is different than a traditional year. In September (specific dates not determined), Agencies will submit a current services budget (M-16-10: *Requirements for the FY 2018 Budget Process*) rather than the typical budget request. OMB is continuing to make efforts to drive alignment between Agencies' overall budget and IT budget submissions. The transition year revised schedule for the FY 2018 Budget Process is listed below:

- Verification that the required E-Gov/LoB contribution levels are being included in the Agency's budget plans: **August 26, 2016**;
- FY 2018 Draft Agency IT Investment Portfolio Summary submission: **September 9, 2016**;
- FY 2018 Draft Agency Budget Accounts Summary submission: **September 9, 2016** for PY only (this should reflect FY 2016 enacted/likely actual level consistent with guidance in A-11 Section 55);
- FY 2018 Agency IT Portfolio Summary submission (including the Agency IT Investment Portfolio Summary, Agency Provisioned IT Spending Summary, Agency Data Center Spending Summary, and Agency Budget Accounts Summary): **September 26-30, 2016**
- FY 2018 Major IT Investment Business Case submissions:
  - For existing major Investments: **October 3-14, 2016** (tentative);
  - For new major Investments, including Security and Compliance Investments: **November 14-18** (tentative);
- Certification of "IT Resource Statements", based on FITARA requirements: **December 1, 2016**; and
- Final FY 2018 President's Budget submissions **(**To Be Determined).

Specifically, a draft version of the Agency IT Investment Portfolio Summary shall be completed by the Agency and submitted to OMB as a Microsoft (MS) Excel file. This draft will constitute the Agency's proposal to OMB, providing a comprehensive list of all IT Investments that will be reported as part of the Agency's FY 2018 IT submission. It also confirms the mapping of Agency Investments to Agency architectures. The initial Draft Agency IT Investment Portfolio Summary is due August 26, 2016 and shall be posted online to the Draft Agency IT Investment Portfolio Summary OMB MAX submission page. Additionally, the Draft Agency Budget Accounts Summary, for PY 2016 only, is due September 2, 2016 and shall be posted online to the Draft Agency Budget Accounts Summary OMB MAX submission page. Specific steps for completing the submissions will be available on the OMB MAX Community Integrated Data Collection (IDC) page. At a minimum, the Draft Agency IT Investment Portfolio Summary should include the Previous Unique Investment Identifier (UII), Current UII, Investment

Category, Shared Services Identifier, Part of Agency IT Portfolio Summary, Type of Investment, Investment Title, Investment Description, and FEA BRM Services – Primary service area.

All subsequent updates to the Agency IT Investment Portfolio Summary will be submitted to the IT Dashboard (ITDB) or as otherwise directed. The Agency IT capital planning office should coordinate and review all versions/revisions of any section/part of the Agency IT Portfolio and Major IT Business Case prior to submission of the Agency Chief Information Officer (CIO) -approved version to OMB.

Additional updates to the Agency IT Portfolio and Major IT Investment Business Cases may be required after final budget decisions, or if the Agency requests supplemental funds that require changes to improve reporting accuracy. Specific instructions and deadlines for submitting updates, corrections, and final submissions of these exhibits will be available on the OMB MAX Community IDC page (as this is typically outside of the regular IDC schedule these will be special instructions on the IDC). If an Agency requests supplemental funds, approves additional funding, or reallocates funding within its authority and these funding changes result in changes to any part of the Agency IT Portfolio Summary, then Agencies should submit a new or revised Agency IT Portfolio Summary as part of their supplemental request.

With reference to the requirements in Circular A-11, Sec. 51.3, CIOs should, in conjunction with their Agency's submission of Current Services baseline budget data, provide the certifications needed to demonstrate compliance with the Federal IT Acquisitions Reform Act (FITARA). Agencies are also required to post a copy of these certifications, hereby termed their "IT Resource Statements", to the following IT Resource Statements (BY 2018) MAX submission page. OMB expects that this copy will be posted no later than, December 1, 2016. For the Final FY 2018 President's Budget, Agencies should update and re-post their IT Resource Statements on the same MAX page. The IT Resource Statements should include: (1) a statement from the CIO affirming that the CIO has reviewed and approved major IT Investments as part of planning budgetary estimates for all years of the Agency's Current Services baseline; (2) a statement from the Chief Financial Officer (CFO) and CIO affirming that the CIO had a significant role in reviewing planned IT support for major programs and significant increases and decreases in IT resources reflected in the Agency's Current Services baseline budget submission, and (3) a statement from the CIO and CFO that the IT Portfolio (Section 55.6) includes appropriate estimates of all IT resources included the Agency's Current Services baseline.

2.2 Quarterly Reporting:
The IDC will be collected based upon the following quarterly submission schedule (separate instructions will be provided 30-45 days before the due date, and the windows for data entry will be longer):

- May 31, 2016; August 31, 2016; November 30, 2016; and February 28, 2017.

2.3 Regular Updates Reporting:

- Major IT Investment updates for performance metrics, risks, projects, and/or activities will be provided to the ITDB as soon as the data becomes available (see Appendix C for a description of major IT Investments).
- CIO Evaluation (per 40 U.S.C. § 11315 (c)(2)) should be updated as soon as CIOs have completed their evaluations. There is no mandated reporting frequency; however, OMB does expect at a minimum that these evaluations will occur each time a TechStat occurs, a rebaseline is approved by the Agency head, when the business cases are submitted to OMB in the Agency budget request, and when the business cases are prepared for the President's Budget release.
- When providing updates to the ITDB, OMB expects that updates are provided within 30 days from the corresponding event (e.g. TechStat sessions, baseline changes, CIO evaluations, status change in projects/activities, status change to the risk information, etc.).

At any given time, when OMB or the Agency CIO, or the Agency Inspector General (IG) determines data reported on the ITDB is not timely and reliable, the CIO (in consultation with the Agency head) must notify their OMB desk officer in writing (via e-mail) and the Agency IG. In addition, within 30 days of this determination, the CIO will collaborate with OMB to develop an improvement plan to address the deficiencies. The plan should include a root cause analysis, timeline to resolve, brief description on how the Agency plans to resolve the issue, and lessons learned. Furthermore, the CIO will communicate the steps being taken to execute the improvement plan and will provide updates on the progress to OMB and the Agency IG on the quarterly basis until the identified deficiency is resolved.

3. How is IT spending categorized?

Agencies are required to submit all of their IT budget-related costs to OMB annually. The Agency's complete IT Portfolio must be reported for all major and non-major IT Investments, including migration-related and funding contributions to IT shared services. The service provider shall report migration-related costs separately to maintain operations for current customers. For the FY 2018 President's Budget submission, IT funding levels reported in the Agency IT Portfolio Summary should be consistent with the Agency's budget materials and should be categorized based upon the following four (4) parts:

Category	Description
Part 1. IT Investments for Mission Delivery	Report IT Investments that directly support the delivery of the Agency's mission. Investments in this part should be listed by the Agency-designated mission delivery areas. This information should map directly to the Agency's strategic and annual performance plan. For IT Investments that cover more than one mission, report in the mission area with oversight over the IT Investment.
Part 2. IT Investments for Administrative Services and Support Systems	Administrative services are comprised of activities that are common across all Agencies and include functional areas such as financial management, human resources, acquisitions, and grants management. Report all Investments for Administrative Services and Support Systems specific to an Agency, and IT Investments officially designated as shared services and E-Gov/ Line of Business (LoB). Per OMB M-16-11, officially designated shared service providers (SSPs) include Agencies previously designated by the Department of Treasury's (Treasury) Office of Financial Innovation and Transformation (FIT), the Office of Personnel Management's (OPM) HR Line of Business (HRLoB) as well as any SSPs designated by the General Services Administration's (GSA) Office of Unified Shared Services Management (USSM). Appendix B provides a list of these Investments, SSPs, and E-Gov/LoBs. Agencies must report IT Investments that are contributing towards an SSP or E-Gov/LoB Investment. The SSPs, including those non-designated by USSM, must report IT Investments made in support of the migration of a customer Agency as well as IT Investment made to support ongoing operations.
Part 3. IT Investments for IT Infrastructure, IT Security, and IT Management	Report IT Investments for IT Infrastructure, IT Security, and IT Management. This section should include all IT Infrastructure, Telecommunications, Hosting, IT Security, End User Services, and all IT Management including CIO and senior leadership for IT strategy and planning, enterprise architecture, capital planning, IT vendor management, and IT budget/finance. For the FY 2018 submission, Agencies must report two standard IT Investments; IT Security and Compliance (as a major) and IT Management (as a non-major). Additional standardized Investments will be required for the FY 2019 cycle. Definitions are included in Appendix C. These Investments should be reported at the point of management and thus may be defined at the bureau level and/or by functional components, or at the Agency level if the Investments are managed for the enterprise. Consequently, there may likely exist more than one of the same type of standard Investment submitted by Agencies, particularly by federated Agencies, that are

Category	Description
	managing standard Investments at lower than the enterprise level.
Part 4. IT Investments for Grants and Other Transferred Funding to Non-Federal Organizations for IT	Report total amounts for grants and other transferred funding to non-federal organizations (i.e. state and local governments) to be used for IT. Part 4 does not relate to Agency grants management systems (reported in Part 2).

Note: National Security Systems (previously Part 5) should be aligned with the appropriate part above, and will be delineated using Investment identifier (02) within column/field 10.

4. If I submitted an Agency IT Portfolio Summary last year, how do I revise it this year?

If the Agency submitted an Agency IT Portfolio Summary for the FY 2017 Budget, the revised FY 2018 Agency IT Investment Portfolio Summary data must be compliant with the FY 2018 specified formats or it will be rejected. The Agency must note "change in status" for each Investment, as compared to the final FY 2017 President's Budget (February 2016 or most recent update). Changes must be identified and described in columns twelve (12) and thirteen (13) of the Agency IT Investment Portfolio Summary.

It is important that the Agency updates its Agency IT Investment Portfolio Summary to reflect current IT Investment data. Note that the PY funding should be updated to reflect the FY 2016 Actuals for the final FY 2018 President's Budget. An OMB Budget Account code for all 'Funding Sources' line items is required for every Investment.

AGENCY IT INVESTMENT PORTFOLIO SUMMARY

The President's Budget Agency IT Portfolio Summary is a complete report of all IT resources within the Agency. Investment costs are to be provided in **millions of dollars ($M)**. Reporting to three (3) decimal places (precision to thousands of dollars) is recommended, although Agencies may report up to six (6) decimal places (whole dollars).

5. What must I report?

The Agency IT Portfolio Summary includes all IT resources for the IT Investments from all funding sources. This means that for each Investment, the Agency must identify the funding source and budgetary resources, including the OMB Budget Account codes, used for the Investment. Agencies should add as many funding source line items as are appropriate for the Investment.

To avoid double-counting or under-counting for E-Gov and/or Multi-Agency collaboration Investments, the total funding source amounts for an Investment must match the Investment line item. To that end, the Agency IT Portfolio Summary of the Investment's managing partner should only include funding from its own Agency in the "Agency Funding" columns and include funds received from partner Agencies in the "Contributions" columns. Likewise, the partner Agency's IT Investment Portfolio Summary should include funding that is being transferred to the managing partner in its own "Agency Funding" columns (using the Investment type: "04-Funding transfer Investments). The Major IT Business Case will include all funding (both from the managing partner's "Agency Funding" as well as the partner Agency's contributions).

Use the following 10-digit number coding system to update or complete your OMB Budget Account identification code information for IT Investment funding sources:

Entry	Description
XXX-xx-xxxx-x	The first three (3) digits are your Agency code (See: Appendix C of OMB Circular No. A-11).
xxx-**XX**-xxxx-x	The next two (2) digits are your bureau code (See: Appendix C of OMB Circular No. A-11). Note: The "bureau" code embedded in the OMB account number for a funding source might not always refer to a "bureau" as the term is used elsewhere.
xxx-xx-**XXXX**-x	This is a four (4) -digit account code for the OMB budget account, as used by the MAX A-11 application where Agency budget offices provide budget information for the Budget Appendix. (See: Section 79.2 of OMB Circular No. A-11).
xxx-xx-xxxx-**X**	This is a single (1) digit Transmittal Code (See: Section 79.2 of OMB Circular No. A-11).

6. How do I complete the Agency IT Investment Portfolio Summary?

Each Investment identified in the Agency's IT Investment Portfolio Summary must have a UII. The first two (2) columns correspond to the Previous UII's and the Current UII's 12-digit coding. Varied identifying information in columns three (3) through eight (8) is used to categorize Investments.

Column /Field	Description
1	**Previous UII** *[12 digits required for all legacy Investments]* This is the identifier depicting Agency code and unique Investment number used to report the Investment in the previous FY 2017 Agency IT Portfolio Summary submission to OMB. Indicating the UII used for a previous submission allows cross-walk and historical analysis spanning FYs. Previous UII is mandatory, with the exception of new Investments. To indicate consolidations/splits/reorganizations, Agencies can provide more than one entry and separate UIIs with commas.
2 **XXX**- xxxxxxxxx xxx- **XXXXXXXXX**	**Current UII** *[12-digit primary key for all Investments]* The Current UII includes an Agency code and a nine-digit unique identifier. Variable information formerly included in the UII of previous years is not part of the UII primary key. The first three (3) digits represent your Agency code (see Appendix C of OMB Circular No. A-11). The last nine (9) digits serve as your unique identifier. This identifier should be system-generated and applied at the Agency level. It will allow Agencies up to one billion unique identifiers to associate with IT Investments. Once used, the unique identifier must be retired from use for any future new Investment and should remain unchanged for any continuing Investment that is not split, consolidated, reorganized. If an IT Investment is retired, discontinued, or merged with another IT Investment, the unique identifier persists with that IT Investment.
3	**Shared Services Category** *[2-digit code] (variable element)* 00: Code for all Investments other than those coded "24", "36"or "48" 24: E-Gov initiatives or an individual Agency's participation in one of the E-Gov/LoB initiatives 36: SSPs (and their customers) previously designated by Treasury's FIT and OPM's HRLoB as well as any providers designated by the USSM. Agency contributions to FMLoB and HRLoB should use code 24, not code 36. 48: Any Multi-Agency (Inter- or Intra-Agency) collaboration or an individual Agency's participation in one of these initiatives. This includes shared services not officially designated by USSM and excludes E-Gov/LoB initiatives and USSM designated shared services.
4	**Shared Services Identifier** *[4-digit code]* These four digits are applicable for all Investments with a Shared Services Category of 24, 36 or 48. A code will be specifically assigned for all E-Gov/LoB and USSM designated shared services in Appendix B, while Agencies should assign their own four (4) -digit unique codes for Multi-Agency initiatives using the "48" shared services category. This code represents the same 4-digit identifier previously provided in the last nine (9) digits of the UII for Investments starting with xxx-99999**XXXX**.
5	**Bureau Code** *[2-digit code] (variable element)* The two digits indicate the bureau code of the Investment (see Appendix C of OMB Circular No. A-11). If this is a department-level or an Agency-wide activity, use "00" as your bureau code. *Note:* This field refers to the bureau with management responsibility for the IT Investment, which may differ from the "bureau" code embedded in OMB budget accounts used when providing funding sources.
6	**Part of Agency IT Portfolio Summary** *[2-digit code] (variable element)* These two digits indicate the four parts of the Agency IT Portfolio Summary: 01: Part 1. IT Investments for Mission Delivery 02: Part 2. IT Investments for Administrative Services and Support Systems 03: Part 3. IT Investments for IT Infrastructure, IT Security, and IT Management 04: Part 4. IT Investments for Grants and Other Transferred Funding to Non-Federal Organizations for Information Technology

Column /Field	Description
7	**Standard IT Infrastructure and Management Category** *[2-digit code]* These two digits indicate the sub-category of Investments identified as Part 3: IT Investments for IT Infrastructure, IT Security, and IT Management. For FY 2018 Agencies must report two standard Investments; IT Security programs should be reflected within an Investment called IT Security & Compliance and use Category 02, and all CIO Function Investments previously reported in Part 3 should be consolidated into a single Investment called IT Management and use Category 03. All other Investments should use the Not Applicable Category 01. OMB intends to introduce additional standard Investments for the FY 2019 cycle. 01: Not Applicable 02: IT Security & Compliance 03: IT Management
8	**Mission Delivery and Management Support Area** *[2-digit code] (variable element)* These two digits indicate the mission delivery and management support areas. Agencies should assign a unique code for each mission delivery and management support area reported. Agencies shall provide a reference table for mission areas to ofcio@omb.eop.gov to correspond to each submission of the IT Portfolio Summary.
9	**Type of Investment** *[2-digit code] (variable element)* These two digits indicate the Agency's type of Investment. Select one of the following two digit codes according to the type of Investment being reported: 01: Major IT Investments 02: Non-major IT Investments 03: IT migration Investment: The portion of a larger asset and for which there is an existing business case for the overall asset. The description of the IT Investment should indicate the UII of the major asset Investment of the managing partner. 04: Funding transfer Investments: These are primarily used to indicate the partner contribution to an Investment in another Agency's IT Investment Portfolio Summary. The description of the IT Investment should indicate the UII of the managing partner Investment. Intra-Agency collaboration should also use this Investment type.
10	**National Security Systems Identifier** *[2-digit code]* These two digits indicate whether the Investment is a National Security System. Select one of the following two digit codes according to the type of Investment being reported: 01: Non-National Security System Investment 02: National Security System Investment
11	**Line Item Descriptor** *[2-digit code] (variable element)* These two digits identify the nature of the "line item" in the Agency IT Portfolio Summary structure. The digits represent the line number in both the XML format used for Agencies on the ITDB and the line number in an equivalent spreadsheet file (CSV or XLS file), for Agencies not on the ITDB: 00: Total Investment title line, structurally the first line for reporting this particular Investment 04: Funding source or appropriation 09: Any subtotal

Column /Field	Description
12	**Change in Investment Status Identifier** *[2-digit code]* This is used when an Investment has a change in status (e.g., downgraded to non-major IT Investment, eliminated, retired, consolidated, split) for the current budget submission relative to the previous budget cycle. The change of status should be indicated with one of the following reasons: 1. Upgraded from non-major to major IT Investment 2. Downgraded from major to non-major IT Investment 3. Split into multiple Investments 4. Consolidation of Investments 5. Reorganization 6. Eliminated by funding 7. Eliminated by split 8. Eliminated by consolidation 9. Eliminated by reorganization 10. New 11. No Change in Status *Note:* For any new Standard IT Infrastructure and Management Investment, new IT Security and Compliance (02) Investment, or new IT Management (03) Investment, use Investment Status Identifier 10 (New). Investments that have been split (Change in Investment Status Identifier 3) must be included in the Agency IT Portfolio Summary, with new UIIs in the Current UII field. Investments that have been consolidated (Change in Investment Status Identifier 4) must include their Previous UII in column 1.
13	**Agency Description of Change in Investment Status** This is used when an indicator has been chosen for "Change in Investment Status" in order to provide a description of the rationale for the change which may include impacted UIIs, specific references to legislative requirements, or governance board decisions and effective dates. *[255 char]*
14	**Investment Title** This is a text field to provide the Investment title. To the extent that they are not part of the name used by the Agency, other identifiers such as bureaus or other numeric codes should not be included as part of an Investment title.
15	**Investment Description** This is a short public-facing description (limited to 255 characters) for each Investment. This description should explain the purpose of the Investment and what program(s) it supports, including the value to the public. The description should be understandable to someone who is not an expert of the Agency. If the Investment is part of a Multi-Agency initiative or another business case, the Agency should describe where that business case is located in the appropriate Agency budget submission (e.g., managing partner UII). For example, if the Investment represents the Agency's participation in an E-Gov or Shared Service initiative, the description should state this information and refer to the Current UII of the managing partner's business case. *[255 char]*
16	**FEA BRM Services – Primary service area** This is the three (3) -digit code that indicates the predominant business function served by the Investment (not necessarily the mission/business of the Agency).BRM version 3.1 contains the current mapping codes. *[3-digit code]*

Column /Field	Description
17	**Cross-Boundary Information Identifier** *[1-digit code]* This is an activity that crosses a bureau or Agency boundary, including information sharing with international, state, local, tribal, industry, or non-governmental organization partners. More information can be found at www.ise.gov. The goal of this question is to quantify efforts to develop and advance interoperability-based shared services and information across distributed and decentralized communities of interest, based on common mission requirements, semantic interoperability requirements, and the need to bridge and enforce security, privacy, and related policy constraints. If the Investment supports reusable, standardized information exchanges leveraging recognized controlled and managed vocabularies; and/or automated approach to federating trust frameworks and enforcing security, privacy and related policy controls (based on National Institute of Standards and Technology (NIST) 800-53) across boundaries Agencies must indicate which of the following are planned to be used or were used: 1. Information Sharing Environment Core Interoperability Framework 2. National Information Exchange Model (NIEM) & the Common Profile 3. Other 4. None *Note:* If the Investment supports both "1" and "2", select "1".
18	**Supports the Anti-Terrorism-Related Information Sharing Environment** *[select all that apply]* This is an activity that supports Agency efforts to develop, integrate, and reuse anti-terrorism-related mission capabilities and technical services. Terrorism-related is defined as terrorism, homeland security, weapons of mass destruction, and crimes with a national security concern. Targeted capabilities are in most instances dual use, meaning that they are integrated into Agency Enterprise Architectures (EAs) to support many or most of an Agencies missions, including but not limited to anti-terrorism-related efforts. More information can be found at www.ise.gov. The goal of this question is to conduct inventory and support reuse and appropriate interoperability across Investments aligned with the anti-terrorism-related ISE. Investment supports: State and Regional Information Sharing Environments (including but not limited to requests for information, deconfliction, national fusion center strategy implementation, and trafficking in persons). 1. Aligning and integrating field-based intelligence and information sharing entities (i.e., Fusion Centers; High Intensity Drug Trafficking Centers; RISS Centers; Joint Terrorism Task Forces; and related entities or task forces) 2. Integration into the Sensitive but Unclassified network federation using the interoperability guidance and criteria promulgated by the SBU Technical Advisory Committee 3. Request for Information, including event or case/subject (or target entity) law enforcement or criminal intelligence deconfliction 4. Alerts, warnings or notifications 5. Law enforcement, homeland security or criminal intelligence incident reporting (including Suspicious Activity Reporting) 6. Other 7. None *Note:* If the Investment supports one or more of these mission areas, indicate which one(s) by listing the corresponding number(s) listed above.
19	**Development, Modernization, and Enhancement (DME) (PY/2016) Agency Funding** *[$M]* This should indicate FY 2016 amount. See definition of DME in Appendix C.

Column /Field	Description
20	**DME (PY/2016) Contributions** *[$M]* This should indicate the FY 2016 amount contributed from other Agencies. See definition of DME in Appendix C. For Funding Transfer Investments (Investment Type "04"), this field should be 0.
21	**DME (CY/2017) Agency Funding** *[$M]* This should indicate FY 2017 amount. See definition of DME in Appendix C.
22	**DME (CY/2017) Contributions** *[$M]* This should indicate the FY 2017 amount contributed from other Agencies. See definition of DME in Appendix C. For Funding Transfer Investments (Investment Type "04"), this field should be 0.
23	**DME (BY/2018) Agency Funding** *[$M]* This should indicate FY 2018 amount. See definition of DME in Appendix C.
24	**DME (BY/2018) Contributions** *[$M]* This should indicate the FY 2018 amount contributed from other Agencies. See definition of DME in Appendix C. For Funding Transfer Investments (Investment Type "04"), this field should be 0.
25	**Operations and Maintenance (O&M) Spending (PY/2016) Agency Funding** *[$M]* This should indicate FY 2016 amount. See definition of O&M in Appendix C.
26	**O&M Spending (PY/2016) Contributions** *[$M]* This should indicate the FY 2016 amount contributed from other Agencies. See definition of O&M in Appendix C. For Funding Transfer Investments (Investment Type "04"), this field should be 0.
27	**O&M Spending (CY/2017) Agency Funding** *[$M]* This should indicate FY 2017 amount. See definition of O&M in Appendix C.
28	**O&M Spending (CY/2017) Contributions** *[$M]* This should indicate the FY 2017 amount contributed from other Agencies. See definition of O&M in Appendix C. For Funding Transfer Investments (Investment Type "04"), this field should be 0.
29	**O&M Spending (BY/2018) Agency Funding** *[$M]* This should indicate FY 2018 amount. See definition of O&M in Appendix C.
30	**O&M Spending (BY/2018) Contributions** *[$M]* This should indicate the FY 2018 amount contributed from other Agencies. See definition of O&M in Appendix C. For Funding Transfer Investments (Investment Type "04"), this field should be 0.
31	**Number of Government Full Time Equivalents (FTEs) (PY/2016)** This is the number of government FTEs included in the PY funding associated with the Investment. This applies to all Investments, both major and non-major. If an FTE's costs are included in the Investment costs for PY, the FTE or portion of the FTE should be reported, regardless of the FTE's role in the Investment (e.g., technical, managerial, functional, or governance).
32	**Total Government FTE Cost (PY/2016)** *[$M]* This is the total PY cost represented by the number of government FTEs associated with the Investment. This applies to all Investments, both major and non-major. If an FTE's costs are included in the Investment costs for PY, the FTE or portion of the FTE should be reported, regardless of the FTE's role in the Investment (e.g., technical, managerial, functional, or governance). FTE cost should reflect the fully loaded cost of government FTEs (as defined by OMB Circular A-76). For major IT Investments, the total FTE costs reported in this field should match the total FTE costs listed on the life cycle cost table in the major business case.

Column /Field	Description
33	**Number of Government FTEs (CY/2017)** This is the number of government FTEs included in the CY funding associated with the Investment. This applies to all Investments, both major and non-major. If an FTE's costs are included in the Investment costs for CY, the FTE or portion of the FTE should be reported, regardless of the FTE's role in the Investment (e.g., technical, managerial, functional, or governance).
34	**Total Government FTE Cost (CY/2017)** *[$M]* This is the total CY cost represented by the number of government FTEs associated with the Investment. This applies to all Investments, both major and non-major. If an FTE's costs are included in the Investment costs for CY, the FTE or portion of the FTE should be reported, regardless of the FTE's role in the Investment (e.g., technical, managerial, functional, or governance). FTE cost should reflect the fully loaded cost of government FTEs (as defined by OMB Circular A-76). For major IT Investments, the total FTE costs reported in this field should match the total FTE costs listed on the life cycle cost table in the major business case.
35	**Number of Government FTEs (BY/2018)** This is the number of government FTEs included in the BY funding associated with the Investment. This applies to all Investments, both major and non-major. If an FTE's costs are included in the Investment costs for BY, the FTE or portion of the FTE should be reported, regardless of the FTE's role in the Investment (e.g., technical, managerial, functional, or governance).
36	**Total Government FTE Cost (BY/2018)** *[$M]* This is the total BY cost represented by the number of government FTEs associated with the Investment. This applies to all Investments, both major and non-major. If an FTE's costs are included in the Investment costs for BY, the FTE or portion of the FTE should be reported, regardless of the FTE's role in the Investment (e.g., technical, managerial, functional, or governance). FTE cost should reflect the fully-loaded cost of government FTEs (as defined by OMB Circular A-76). For major IT Investments, the total FTE costs reported in this field should match the total FTE costs listed on the life cycle cost table in the major business case.
37	**Functional/Business Sponsor Name** The Functional/Business Sponsor is defined in Appendix C, and provides visibility for Agencies and OMB as to who the sponsor is for each Investment within the IT portfolio.
38	**Functional/Business Sponsor Title** Indicate the title of the Functional/Business Sponsor.
39	**Cloud Computing Alternatives Evaluation** *[one-digit code]* This specifies whether, as of the date of the submission, the Investment, or a component of the Investment, is leveraging, considering, migrating or posing as a candidate for cloud computing. All Investments should answer this question regardless of the overall life cycle stage of the Investment, as operational Investments should consider cloud computing alternatives during or as a result of an operational analysis. Select one of the following answers: 1. This Investment or a portion of this Investment is leveraging cloud computing. 2. This Investment is migrating to the cloud. 3. This Investment is considering cloud computing. 4. Cloud computing has NOT been considered. 5. Cloud computing is NOT applicable for any portion of this Investment. 6. Cloud computing has been considered but was not selected. *Note:* For Funding Transfer Investments (Investment Type "04"), this field does not need to be completed.

Column /Field	Description
40	**DME Provisioned IT Services Spending (PY/2016) Agency Funding** *[$M]* This should indicate FY 2016 amount. See definitions of Provisioned IT Services Spending in Appendix C. This should include Agency funding to outside Agency providers.
41	**DME Provisioned IT Services Spending (PY/2016) Contributions** *[$M]* This should indicate FY 2016 amount. See definitions of Provisioned IT Services Spending in Appendix C. This should include Inter-Agency contributions from other Agencies and Intra-Agency from within the Agency.
42	**DME Provisioned IT Services Spending (CY/2017) Agency Funding** *[$M]* This should indicate FY 2017 amount. See definitions of Provisioned IT Services Spending in Appendix C. This should include Agency funding to outside Agency providers.
43	**DME Provisioned IT Services Spending (CY/2017) Contributions** *[$M]* This should indicate FY 2017 amount. See definitions of Provisioned IT Services Spending in Appendix C. This should include Inter-Agency contributions from other Agencies and Intra-Agency from within the Agency.
44	**DME Provisioned IT Services Spending (BY/2018) Agency Funding** *[$M]* This should indicate FY 2018 amount. See definitions of Provisioned IT Services Spending in Appendix C. This should include Agency funding to outside Agency providers.
45	**DME Provisioned IT Services Spending (BY/2018) Contributions** *[$M]* This should indicate FY 2018 amount. See definitions of Provisioned IT Services Spending in Appendix C. This should include Inter-Agency contributions from other Agencies and Intra-Agency from within the Agency.
46	**O&M Provisioned IT Services Spending (PY/2016) Agency Funding** *[$M]* This should indicate FY 2016 amount. See definitions of Provisioned IT Services Spending in Appendix C. This should include Agency funding to outside Agency providers.
47	**O&M Provisioned IT Services Spending (PY/2016) Contributions** *[$M]* This should indicate FY 2016 amount. See definitions of Provisioned IT Services Spending in Appendix C. This should include inter-Agency contributions from other Agencies and intra-Agency from within the Agency.
48	**O&M Provisioned IT Services Spending (CY/2017) Agency Funding** *[$M]* This should indicate FY 2017 amount. See definitions of Provisioned IT Services Spending in Appendix C. This should include Agency funding to outside Agency providers.
49	**O&M Provisioned IT Services Spending (CY/2017) Contributions** *[$M]* This should indicate FY 2017 amount. See definitions of Provisioned IT Services Spending in Appendix C. This should include Inter-Agency contributions from other Agencies and intra-Agency from within the Agency.
50	**O&M Provisioned IT Services Spending (BY/2018) Agency Funding** *[$M]* This should indicate FY 2018 amount. See definitions of Provisioned IT Services Spending in Appendix C. This should include Agency funding to outside Agency providers.
51	**O&M Provisioned IT Services Spending (BY/2018) Contributions** *[$M]* This should indicate FY 2018 amount. See definitions of Provisioned IT Services Spending in Appendix C. This should include inter-Agency contributions from other Agencies and intra-Agency from within the Agency.

Column /Field	Description
52	**Total IT Security Spending (PY/2016) Agency Funding** *[$M]* This should indicate the FY 2016 security costs associated with each IT Investment. All Investments should report the total cost for IT security within the Investment. For major IT Security and Compliance Investments the total Investment cost and total security cost will likely match. The intent is to capture the security costs specific to the Investment that are not captured within the IT Security and Compliance Investments costs.
53	**Total IT Security Spending (CY/2017) Agency Funding** *[$M]* This should indicate the FY 2017 security costs associated with each IT Investment. All Investments should report the total cost for IT security within the Investment. For major IT Security and Compliance Investments the total Investment cost and total security cost will likely match. The intent is to capture the security costs specific to the Investment that are not captured within the IT Security and Compliance Investments costs.
54	**Total IT Security Spending (BY/2018) Agency Funding** *[$M]* This should indicate the FY 2018 security costs associated with each IT Investment. All Investments should report the total cost for IT security within the Investment. For major IT Security and Compliance Investments the total Investment cost and total security cost will likely match. The intent is to capture the security costs specific to the Investment that are not captured within the IT Security and Compliance Investments costs.
55	**End of Life Spending (CY/2017)** *[$M]* For Investments that include any component; technology, application, or infrastructure, that is end-of-life, this amount should correspond to the amount currently being spent (in the CY). This should include both Agency funding and funds contributed to this Investment. This is not applicable to Funding Transfer Investments (Investment Type "04"). See end of life definition in Appendix C.

AGENCY PROVISIONED IT SERVICES SPENDING SUMMARY

7. How do I report the Agency Provisioned IT Services Spending Summary?

The Agency Provisioned IT Services Spending Summary is to be completed at the Agency level, not at the individual Investment level. Note that the sum of each year should match the sum of the applicable columns 40 to 51 of the Agency IT Portfolio Summary. Only costs directly attributable to cloud computing implementation, operations, or services should be reported into the cloud computer portion of the table below. This may only be a portion of the total cost of contributing/associated Investments. For definitions of terms used, see NIST Special Publication 800-146.

Agency costs for Provisioned IT Services by cloud computing deployment model, by year *[$M]*

- ***Public Cloud*** portion of all Agency cloud computing spending
- ***Private Cloud*** portion of all Agency cloud computing spending
- ***Community Cloud*** portion of all Agency cloud computing spending
- ***Hybrid Cloud*** portion of all Agency cloud computing spending

Note: The "Other Provisioned Services (non-cloud)" category should include all non-cloud Agency-managed provisioned services costs by year.

Cloud Category	PY (FY 2016)	CY (FY 2017)	BY (FY 2018)
Public Cloud			
Private Cloud			
Community Cloud			
Hybrid Cloud			
Other Provisioned Services (non-cloud)			

AGENCY DATA CENTER SPENDING SUMMARY

8. How do I report the Agency Data Center Spending Summary table?

For the upcoming submission, the Agency Data Center Spending Summary table is being adjusted to simply collect the funding levels associated with data centers in order to inform the Data Center Optimization Initiative reporting metrics. This is to be completed for costs that the Agency incurs for data center assets that the Agency owns and operates or obtains via services (i.e., where the infrastructure is neither owned nor operated by the Agency but is procured via a services arrangement). It should include all of the infrastructure reported in Part 3 as well as the infrastructure used to support Investments in the rest of the Agency IT Portfolio Summary (Parts 1 and 2). Each row is mutually exclusive of the others.

IT Infrastructure spending remains a high priority and will continue to be a focus. The intent is to fully eliminate this Summary next year, as the intent is for standard IT Investments to exist for all IT Portfolio Summary Part 3 spending. This year standard Investments for IT Security and Compliance and IT Management are being introduced. Next year, standard Investments for physical and virtual IT infrastructure that span Part 3 in its entirety will be introduced. These new standard Investments will be communicated prior to next year's guidance release so that Agencies have time to adjust and report accordingly. OMB is cognizant that in order for Agencies to shift the way IT costs are reported, existing requirements need to be relaxed to free up time to implement changes and provide the most accurate data possible, which is why the reporting requirement for this Summary has been reduced. Agencies should continue capturing their IT costs in whatever Investment structure they have currently in place and, once standard Investments are identified, put a migration strategy in place to be able to report against the standard Investments for the FY 2019 cycle.

Data Center Cost Category	Total PY ($M)	Total CY ($M)
Data Center Labor		
Data Center Software		
Data Center Hardware		
Data Center Electricity		
Data Center Facility		

Definitions	
Data Center Labor	**Data Center Labor costs <u>include</u>** all costs of government FTEs (as defined by OMB Circular A-76) and contracted personnel associated with the operations and maintenance of a data center. If the responsibilities are a fraction of a person's or several persons' time, report the portion of the individuals' salary multiplied by the fraction of their time spend working on data center activities. **In-sourced staff:** Labor costs include salary, overtime pay, benefits, and "other" employee costs such as job-related travel. Costs for Information Security training, however, should be excluded, as should costs associated with reductions in workforce, relocations, or retirement. **Contractor resources:** Labor costs include the total spending for contractor staff that is supplemental to the Agency staff and "operationally" managed by the in-house staff. For labor associated with outsourced services, spending details by category might not be available. In these cases, those costs should be reported under a "services" category.
Data Center Software	**Data Center Software costs <u>include</u>** server operating systems (both physical and virtual); virtualization and partitioning software; database and data management software; software dedicated to managing and maintaining storage systems; middleware; security software; IT

Definitions	
	management software; messaging and collaboration software; and software-related costs linked to planning, testing, quality control and quality assurance, and implementing disaster recovery. **Data Center Software costs <u>exclude</u>** application software and virtual desktops or VDI.
Data Center Hardware	**Data Center Hardware costs <u>include</u>** processors, storage devices, print devices, tape devices and other peripherals associated with mainframes and servers; as well as other miscellaneous devices needed to support the processing equipment including desktops, laptops, and mobile devices used by personnel supporting the data centers. **Data Center Hardware costs <u>exclude</u>** circuit or similar costs needed to connect to the network, costs for networking equipment (e.g., routers, switches, hubs, firewalls, and monitoring equipment), and costs to connect multiple data centers or processors/devices to each other.
Data Center Electricity	**Data Center Electricity costs <u>include</u>** all electricity used to power data center operations (e.g., servers, environmental, HVAC, lighting). For small data processing environments, Agencies may estimate Data Center Electricity costs by computing electrical costs per square foot and multiplying by the number of square feet of the data processing environment, or by any other consistent, repeatable, justifiable method.
Data Center Facility	**Data Center Facility costs <u>include</u>**: **Costs for IT equipment floor space** (e.g., raised and no-raised floor space used for IT equipment). This is often calculated as the size of the floor space (square footage) multiplied by the monthly rate for that space × 12. **Costs for office and/or other floor space:** This captures the cost for the office space and/or other areas considered part of the data center that is not part of the raised floor space. This is often calculated as the amount of floor space in the data center minus the amount used for IT equipment, multiplied by the monthly rate for that space × 12. **Costs for other facility mechanicals and equipment:** These include costs for the Uninterruptible Power Supply (UPS), redundant power supplies, air conditioning/cooling equipment, power distribution equipment, generators, fuel, and cage access control devices.

AGENCY BUDGET ACCOUNTS SUMMARY

9. How do I report the Agency Budget Accounts Summary?

The Agency Budget Accounts Summary provides an orientation of IT funding levels associated with Budget Accounts/Funding Sources listed for each IT Investment in the Agency IT Investment Portfolio Summary. This summary focusing on the Budget Accounts orientation serves as a tool for Agency CIOs and CFOs to collaborate and jointly certify the Agency's IT submissions. To support FITARA implementation and drive increased CIO authorities, the intent is that the IT funding dollar amount that the CIO has direct authority over within each Budget Account will increase over time.

The Agency Budget Accounts Summary is to be completed at the Agency level (NOT at the individual Investment level) for the PY, CY and the BY. It should include all budget accounts that fund IT across the entire Agency, comprehensive of all component level organizations, for Agency funding only, not the amounts included in contribution funding columns in the Agency IT Investment Portfolio Summary. While budget account codes are listed within each IT Investment, this table summarizes the total IT funding levels within each account and the CIO's authority for each. For the CIO Authority column, a dollar amount should be entered depicting the amount within the BY that the Agency CIO (not a component-level CIO) has direct authority over and decision making authority over, within the total IT funding level listed for each budget account. The amounts should include all funding sources (see the definition of Funding Sources in Appendix C) that are spent on IT, including FTEs and Provisioned IT services. The combined Agency total funding (DME and O&M) for each year in this table should be the same as the Agency total funding in the IT Investment Portfolio Summary for the same years.

Budget Account Code	**CIO Authority (in dollar value for BY)**	**PY 2016**		**CY 2017**		**BY 2018**	
		DME	O&M	DME	O&M	DME	O&M

MAJOR IT BUSINESS CASE

10. What is the purpose of this guidance?

OMB provides specific policy, procedural, and analytic guidelines for planning, budgeting, acquisition, and management of major IT capital Investments in addition to general guidance issued in OMB Circular No. A-11 and OMB Circular No. A-130.

The Agency IT Portfolio Summary and Major IT Business Cases (including Business Case and Business Case Detail) describe the justification, planning, and implementation of an individual capital asset included in the Agency IT Portfolio Summary and serve as key artifacts of the Agency's EA and IT Capital Planning and Investment Control (CPIC) processes.

Together, the Major IT Business Case and Major IT Business Case Details provide the budgetary and management information necessary for sound planning, management, and governance of major IT Investments. These documents help Agencies explicitly align IT Investments with strategic and performance goals, and ultimately provide value to the public by making Investment and management information more transparent. As architecture-driven IT Investments are funded in the "Select" CPIC phase, they move forward into the implementation phase. The system development life cycle processes are then followed and actual outputs, schedule, and operational performance expenditures are tracked against planned numbers using performance-based management processes as part of the CPIC "Control" Phase.

11. How will Agencies manage IT capital assets/Investments?

There are three (3) primary OMB Circulars that describe the complete set of requirements regarding the management of IT resources.

1. The Capital Programming Guide of OMB Circular No. A-11 provides guidance on the principles and techniques for effective capital programming.
2. OMB Circular No. A-11, Appendix J explains the principles of financing capital asset acquisitions.
3. OMB Circular No. A-130 establishes additional requirements for EAs, planning and control of information systems and IT Investments, IT Governance, and performance management.

These requirements include but are not limited to the following objectives of the CPIC processes for their portfolio of IT resources:

- Implement the strategies and requirements of and manage the full scope of decisions related to all Agencies' IT described in FITARA, Title VIII Subtitle D of the National Defense Authorization Act (NDAA) for Fiscal Year 2015, Pub. L. No. 113-291.

- Ensure that the planning and management of Agency IT resources fully implement the requirements of OMB Circular No. A-130, "Management of Federal Information Resources."

- Ensure that covered Agencies shall continue to provide information to the ITDB, as detailed within this guidance, which is issued annually in conjunction with the release of OMB Circular A-11. As a part of that guidance, Agency engagements including PortfolioStat, FedStat, OMB and/or Agency-led TechStat reviews, and Desk Officer Reviews will be used to meet FITARA requirements. Per OMB M-15-14:

- TechStat Sessions - A TechStat is a face-to-face, evidence-based accountability review of an IT program with Agency leadership. TechStat sessions are a tool for getting ahead of critical problems in an Investment, turning around underperforming Investments, or terminating Investments if appropriate. For all Agency-led TechStat reviews of Investments, the Agency shall contact ofcio@omb.eop.gov with the subject line, "[Agency Acronym] TechStat Notification," at least two weeks ahead of the TechStat session. Agencies shall follow the Agency's TechStat policy and procedures based on the CIO.gov TechStat Toolkit when managing TechStat sessions. Agencies shall report the outcomes and outputs of all TechStat sessions quarterly, to include a root cause analysis of performance issues, corrective action plans which address these causes, and a timeline for implementing the corrective actions. More detailed reporting guidance is included in the quarterly IDC instructions.

- Evaluate and select capital assets that will support core mission functions performed by the Federal Government and that demonstrate projected returns on Investment that are clearly equal to or better than alternative uses of available public resources. Specifically for IT, the Investments should be informed by and should address performance gaps and goals identified in an Agency's strategic plan, annual performance plan, and EA.

- Initiate improvement to existing assets or acquisition of new assets only after considering alternative private sector or governmental source solutions. .

- Implement IT reforms based upon current guidance and best practices such as U.S. Digital Service Playbook, TechFAR, modular development guidance, Investment and forthcoming agile development guidance.

- Assign an Agency functional/business sponsor (separate from the PM) for each Investment who is responsible for the program or function supported or implemented by the Investment. The sponsor is responsible for expressing the value of, ensuring successful implementation of, and providing accurate and timely data for the IT Investment to the Agency CIO and OMB. Each major and non-major IT Investment listed in Agency IT Portfolio Summary must include the name of the functional/business sponsor name and title.

- Encourage agile development whenever possible to ensure that solutions are delivered using an iterative approach through close collaboration with product owners and business sponsors who are embedded in agile teams which allows for frequent reassessment in an incremental manner.

- Encourage agile development and digitization where ever possible. Digitization is an alternative delivery method to automation. "digitization" is purposely and deliberately differentiated from "automation," a process which has been underway for decades.

  - Automation can be characterized as the use of information technology to speed up existing business processes and interactions, and often can bring significant computing power to assist in performing tasks which would otherwise require excessive amounts of labor and resources. Examples of automation include payroll processing, performing bookkeeping and financial calculations, and even first and second generation web forms that largely mirror the paper forms and business practices upon which they were originally based.

- Digitization is fundamentally different from automation in that one of its core premises is to prioritize customer experience and in doing so, erases the traditional barriers to information access that are bound to outdated architecture such as human organization structures, physical storage of data, or business process constraints. Another core premise of automation is that the

power of information technology and the use of user and ecosystem interaction data can, and should be harnessed to redefine, optimize, and personalize the experiences by which agencies interact both internally and externally. Quite often, digitization harnesses newer forms of technology (such as mobile, sensors, social media, metadata, shared services, etc.) to deliver a differentiated and personalized end-user experience. Reduce project risk by avoiding or isolating custom-designed components, using components that can be fully tested or prototyped prior to full implementation or production, and ensuring involvement and support of users in the asset design and testing of the asset.

- Structure major planning and acquisition into useful segments with a narrow scope and brief duration. These segments should make adequate use of competition and appropriately allocate risk between the Federal Government and the contractor. The Agency CIO must approve or define the cost, schedule, and performance goals for major acquisitions, and the Agency's CFO must evaluate the proposed cost goals.

- Based on the Agency Information Resources Management (IRM) Strategic Plan, Agency leadership will ensure a continuous linkage between Federal, Agency, and bureau EAs, demonstrating such consistency through alignment with the Agency's Enterprise Roadmap and target architecture, compliance with Agency business requirements and standards, as well as identification of milestones, as defined in the Agency's EA transition strategy.

- Institute performance measures and management processes to monitor and compare actual performance to planned results. Each methodology should have a set of measures that are consistent, appropriate, and tailored to that methodology.

- Achieve, on average, 90 percent of Agency cost, schedule, and performance goals for major acquisitions, per requirements of Federal Acquisition Streamlining Act of 1994 (FASA, Title V). Through the TechStat process and as part of the Clinger-Cohen Act responsibility, Agency Heads should review major acquisitions that have not achieved 90 percent of the goals to determine whether there is a continuing need and what corrective action, including termination, should be taken.

- Ensure that Agencies' financial management systems conform to the requirements of OMB Circular No. A-127.

- Conduct post-implementation or post-occupancy reviews of capital programming and acquisition processes and projects to validate estimated costs and benefits and to document effective management practices (e.g., lessons learned) for broader use.

- Establish oversight mechanisms that require periodic review of operational capital assets to determine how mission requirements might have changed and whether the asset continues to fulfill ongoing and anticipated mission requirements, deliver intended benefits to the Agency and customers, and meet user requirements.

- Develop, maintain, and submit within five (5) business days (upon OMB request) the following Investment artifacts for all major IT Investments, as applicable:

    - Risk management plan and risk register
    - Investment charter, including IPT
    - Investment-level alternative analysis and benefit-cost analysis
    - Operational analyses (for operational and mixed life cycle systems)
    - Post implementation review results (Investment level or project-specific)

- Documentation of Investment re-baseline management approval(s)
- Documentation/justification of an Investment's elimination due to funding, consolidation, reorganization, or split

Note: Specific artifacts for Security and Compliance Investments have not been specified.

12. What is the CIO Evaluation?

Provide CIO numeric evaluation (1-5) for all major IT Investments that reflect the CIO's best judgment of the current level of risk for the Investment in terms of its ability to accomplish its goals (per 40 U.S.C. § 11315 (c)(2)). The evaluation could be informed by the following factors, including but not limited to: risk management, requirements management, contractor oversight, historical performance, human capital, and other factors that the CIO deems important to forecasting future success. CIOs should consult with appropriate stakeholders (e.g. Chief Acquisition Officers, program managers, customers, etc.) in making their evaluation. Each evaluation should include a narrative explanation when the numerical rating has changed since the last evaluation; and a numeric rating based on the aforementioned factors.

The following factors and supporting examples can be used to inform the CIO Evaluation:

Evaluation Factor	Supporting Examples
Risk Management	• Risks and associated impact are well understood by senior leadership. • Risk log is current and complete. • Risks are clearly prioritized. • Mitigation plans are in place to address risks. • Change control is established and communicated to all stakeholders (especially with system and process dependencies). *Note*: Risk management implies that active risks are being managed and mitigated accordingly. Active risks include, but are not limited to funding cuts and staffing changes.
Requirements Management	• Investment objectives are clear and scope is controlled. • Requirements are clear and validated. • Stakeholders are actively involved in the requirements process per appropriate methodology. • Product backlog is prioritized periodically based on recent release and stakeholder feedback.
Contractor Oversight	• Acquisition strategy is defined and managed via an Integrated Program/Project Team. • Agency receives key reports, such as earned value, current status, and risk logs. • Agency is providing appropriate management of contractors such that the government is monitoring, controlling, and mitigating the impact of any adverse contract performance.
Performance	• No significant projected deviations from planned cost, schedule, scope, and value metrics. • Lessons learned and best practices are incorporated and adopted.
Human Capital	• Qualified management and execution team for the IT Investments and/or contracts supporting the Investment. • Low turnover rate and hiring contingency in place.
Other	• Other factors that the CIO deems important to forecasting future success.

13. What other requirements does the Major IT Business Case Detail fulfill?

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. The Major IT Business Case should demonstrate support for the mission statements, long-term goals and objectives, and annual performance plans developed pursuant to the Government Performance and Results Act – Modernization Act (GPRA-MA) of 2010. Major IT Business Case Detail on Major IT Investments establishes reporting requirements through the ITDB to ensure the proper execution of those Investments against the established performance plans. The IT Security and Compliance Investment data informs Agency leadership and OMB on the IT Security risk posture and the IT Security spend on Agency IT Security programs.

14. What must I report in the Major IT Business Case and Major IT Business Case Detail, and when?

The policy and budget justification principles in the Major IT Business Case and Major IT Business Case Details apply to all Agencies of the Executive Branch of the Federal Government that are subject to Executive Branch review (see Clinger-Cohen Act of 1996). Section 25 of OMB Circular No. A-11 details this authority to collect and review Business Cases for Major IT Investments.

All information necessary to complete the Major IT Business Case and Major IT Business Case Detail should already exist as part of the Agency's overall capital planning activities and within project- and program-specific documentation. The materials used to populate Major IT Business Case and Major IT Business Case Detail should be readily available to OMB upon request.

Additional information on the submission process will be posted on the OMB MAX Community IDC page. As always, pre-decisional, IT security-sensitive, and procurement-sensitive information will not be displayed to the public.

All software development projects must produce usable functionality at intervals of no more than six (6) months. All major development projects within Investments are required to use modular/agile development principles.

Major IT Business Case Details on major IT Investments shall establish cost, schedule, and performance targets for PY and CY.

Periodic performance metrics updates for ongoing operations will vary according to the nature of the metric, as indicated in Table C1.A.

For major Investments designated as IT Security and Compliance Standard Investments (code "02" in Column 7 of the IT Investment Portfolio Summary), complete Major IT Business Case Section D and F only. For major Investments not designated as an IT Security and Compliance Standard Investment (codes "01" or "03" in Column 7 of the IT Investment Portfolio Summary), complete both the Major IT Business Case Sections A through D and Major IT Business Case Details sections A through C. For Investments designated as Administrative Services and Support Systems Investments (code "02" in Column 6 of the IT Investment Portfolio Summary) complete both the Major IT Business Case Sections A-E and Major IT Business Case Details sections A-C (see MAJOR IT BUSINESS CASE table on page 3).

15. How will Multi-Agency Collaboration and Intra-Agency Shared Services Investments be captured in the Major IT Business Case and Major IT Business Case Detail?

The managing partners (lead Agency that provides services or coordination services to other Agencies or other units within their Agency) will take the lead in completing and submitting the Multi-Agency collaboration or Intra-Agency shared services Major IT Business Case and Major IT Business Case Detail, managing it through the managing partner's capital programming and budget process. The managing partner for Multi-Agency or Intra-Agency collaboration Investments is also responsible for ensuring that the Investment is included in the their Agency IT Portfolio Summary. It should include all necessary information from the partner Agencies (customers who receive services from the managing partners) and should have been approved by all necessary partner organizations through the appropriate governance process.

Specifically, the tracking of partner Agency funding, and related capital assets (e.g., migration Investments, Centers of Excellence, Shared Service Providers, supporting components) for Government-wide E-Gov and Line of Business Investments, will be captured via the OMB MAX Funding Tool for E-Gov-LoB Initiatives. Managing Partners for Government-wide E-Gov/ LoB Investments listed in Appendix B are required to submit Major IT Business Cases unless they obtain a waiver from OMB.

Shared Service Providers are required to submit Major IT Business Cases using the UIIs listed in Appendix B. Agencies with significant Investments in financial management, human resources, grants, or acquisitions systems, and/or services that would either provide new or modify existing capabilities to be used government-wide or that would duplicate those already available are required to submit a Major IT Business Case. To help guide OMB funding determinations, the USSM will provide recommendations to OMB on whether customer and provider strategies align with the government-wide shared service approach. When an Agency selects a USSM designated Shared Service Provider for migration, the lead in completing and submitting the Major IT Business Case will switch from the customer to the provider. The provider is responsible for coordinating with the customer to provide the total cost of migration. The customer Agency will still include this Investment in their Agency IT Portfolio Summary and reference the Current UII of the provider Agency in the "Investment Description" field.

During the development of the shared services Major IT Business Case and Major IT Business Case Detail, Agencies are encouraged to utilize the USSM M3 Playbook. The M3 Playbook was created using leading practices and lessons learned from previous migration efforts to increase the likelihood of successful migrations. The USSM will monitor Investments to ensure Agencies are following the disciplined processes outlined in the M3 Playbook and assess project risk in partnership with OMB. Agencies are encouraged to submit the documentation identified in the M3 Playbook for each phase of the Investment for review. High risk Investment as identified by the USSM in partnership with OMB will be required to receive approval from OMB prior to advancing to the next phase as identified in the M3 Playbook. OMB may require additional information related to these Investments and will work with the customer and provider Agencies to coordinate data requests.

Partner Agencies should reference the name and Current UII of the Multi-Agency/Intra-Agency shared services Investment in the "Investment Description" field of their own partner Agency IT Portfolio Summary. Partner Agencies should also ensure their activities and participation are included in the appropriate sections of the Multi-Agency Major IT Business Case. The entire Life Cycle Cost total for the Investment, including funds provided by partner Agencies, should be included in the Multi-Agency Collaboration or Intra-Agency Shared Services Investments Business Case.

Investments that provide a service to other Agencies but do not receive contributions from partner Agencies should be reported as Multi-Agency Collaboration Investments.

Investments for Multi-Agency collaboration, shared services, and/or LoBs will be reflected in the managing partner's annual Enterprise Roadmap submission to OMB.

Managing partners that provide Multi-Agency services should ensure that funding is prioritized to accommodate building and obtaining approval of a shared architecture. Approval should be obtained through a working governance model that includes partner Agencies, customers, and OMB.

OMB may require additional information from partner Agencies related to the Multi-Agency collaboration Major IT Investments. When necessary, OMB will work with the managing partners to coordinate data requests.

16. How will OMB use the Major IT Business Cases?

The Major IT Business Case is one component of the Agency's total budget justification (see Section 51.2 of OMB Circular No. A-11). OMB uses data reported in the Major IT Business Case to make quantitative decisions about budgetary resources consistent with the Administration's program priorities as well as qualitative assessments about whether the Agency's programming processes are consistent with OMB policies and guidance. OMB may request additional supporting information from Agencies as necessary.

17. What fields are included and how do I complete the Major IT Business Case?

Each Investment identified in the Major IT Business Case must have a UII. The Major IT Business Case captures data on the strategic relevance, planning, budgeting, and technical capability for Agency Major IT Investments. Section A refers to the Investment UII's 12-digit coding. Section B includes additional fields concerning how the Investment relates to and supports the Agency mission, its cost effectiveness, and a description of leadership. Section C includes fields relevant to Investment past, current, and out-year budgeting. Section D concerns Investment current and planned contract acquisition strategy. Section E includes fields for capturing Systems data for Administrative Services and Support Systems IT Investments. Section F pertains to Cost and Capabilities data for Agency IT Security and Compliance Standard Investments. Agencies should complete relevant sections based on the type of Major IT Investment as described in that chart on page 3.

The following are the sections of the Major IT Business Case:

Section A: General Information	
Column /Field	**Description**
1	**Investment Name** *Note:* This field will be auto-populated from the Agency IT Portfolio Summary.
2	**UII (12-digit primary key for all Investments)**

Section B: Investment Detail	
Column /Field	**Description**
1	Briefly describe the Investment's purpose, goals, and current or anticipated benefits (quantitative and/or qualitative). Include the Investment's specific contribution to mission delivery or Agency management support functions and identify key customers, stakeholders, and other beneficiaries. *[2500 char]*
2	Provide at least one Agency Strategic objective code (A-11 Section 230) and/or Agency Priority Goal code (A-11 Section 250) that this Investment aligns to on performance.gov. If this Investment aligns to more than one Agency strategic objective code and/or Agency Priority goal code list all that apply. If your Agency does not report to performance.gov please use "0". You may locate the full list of current Agency Strategic objective codes by downloading the spreadsheet available on performance.gov. *[5 digits]*
3	Briefly describe the Investment's return on Investment, including benefits (internal and external to the government), and outcomes achieved or planned. *[2500 char]*

Section B: Investment Detail	
Column /Field	**Description**
4	Provide specific requirements for this Investment (i.e. legislative mandates, outstanding audit findings or material weakness, Presidential Directive) and how this Investment will meet the requirement. Additionally, provide any applicable URLs to associated requirements. *[2500 char]*
5	Identify the foremost program supported by this Investment, using the Program Code in the Federal Program Inventory Reference Table. If this Investment does not primarily support a single program (e.g. provides Department-wide infrastructure, or supports multiple programs evenly), enter "No Primary Program". *[XXX-XXX or "000-000" for "No Primary Program"]*
6	If this Investment eliminates or reduces another major or non-major IT Investment(s), please list the Investment(s) and their status as represented below. (Eliminated or reduced Investments should be listed until removed from the Agency's IT Investment Portfolio Summary. Most eliminated Investments should remain in the Agency's IT Investment Portfolio Summary for two years.)

	Investment UII(s)	***[12-digit UII]***
	To Be Status	*[to be eliminated/to be reduced]*
7	Does the Investment include:	
	A shared service (Intra- or Inter-Agency—current and/or planned)?	*[Yes/No]*
	Are all systems in this Investment PIV-enabled systems (per HSPD-12 and OMB Memorandum M-11-11)?	*[Yes/No]*
8	**Public URL(s):** Provide any public facing URLs associated with this Investment, including APIs (if applicable). List as many URLs as apply, https://…	
9	**PM Name:** Provide the name of the Investment-level project manager. *[250 char]*	
10	**PM Email:** Provide the e-mail of the Investment level project manager. *[250 char]*	
11	**PM Qualifications** The qualification/experience level of the PM (per OMB M-04-19). Select one of the following: FAC-P/PM(DAWIA-3) – Senior FAC-P/PM(DAWIA-2) – Mid-Level FAC-P/PM(DAWIA-1) – Entry Level Other certification with 4 or more years of PM experience (within the last five years) Other certification with between 2 and 4 years of PM experience (within the last five years) Other certification with less than two years of PM experience (within the last five years) No certification, but with 4 or more years of PM experience (within the last five years) No certification, but with between 2 and 4 years of PM experience (within the last five years) No certification, but with less than two years of PM experience (within the last five years	

Section C: Life Cycle Costs

Provide the total estimated life cycle cost for this Investment by completing the following table. All totals represent all IT resources and budgetary sources of funding, consistent with the Agency IT Portfolio Summary. Totals are to be reported in **millions of dollars**. Variations from planned expenditures will be reflected in Tables B.2.1 and B.2.2 in the Major IT Business Case Detail. Federal personnel costs should be included only in the rows designated as "… Govt. FTE costs" and should be excluded from other costs.

For Multi-Agency Investments, this table should include all funding (both managing and partner Agency contributions), and subsequently may not match figures provided in the Agency IT Portfolio Summary.

To the degree possible, the costs associated with the entire life cycle of the Investment should be included in this table. Whether solutions being developed in an agile fashion or other development methodology, for years beyond BY+1, please provide your best estimates for planning purposes, understanding that estimates for out-year spending will be less certain than estimates for BY+1 or earlier.

For lines in the table that ask for changes in your current submission compared to your most recent previous submission, please use the FY 2017 President's Budget as your previous submission. When making comparisons, please ensure that you compare same-year-to-same-year (e.g., the FY16 level for 2016 versus the FY17 level for 2016). Significant changes from the previous submission should be reflected in an updated Investment-level Alternatives Analysis, subject to OMB review.

Note: Do not enter information for the dark gray cells (these will be calculated).

	PY-1 & Prior	PY 2016	CY 2017	BY 2018	BY+1 2019	BY+2 2020	BY+3 2021	BY+4 & Beyond
Planning Costs								
DME (Excluding Planning) Costs								
DME (Including Planning) Govt. FTE Costs								
Sub-Total DME (Including Govt. FTE Costs)								
O&M Costs								
O&M Govt. FTE Costs								
Sub-Total O&M Costs (Including Govt. FTE Costs)								
Total Cost (Including Govt. FTE Costs)								
Total Govt. FTE costs								
Number of FTE rep by costs								
Total change from PY final President's Budget ($)								
Total change from PY Final President's Budget (%)								

Table/Field	Description
2.a.	In which year did or will this Investment begin? *[YYYY]* *Specify a year, e.g. PY-1 = 2015*
2.b.	In which year will this Investment reach the end of its estimated useful life? *[YYYY]* *Specify a year, e.g. BY+5 = 2023*
3	Compare the funding levels for PY and CY to the final FY 2017 President's Budget for those same years. Briefly explain any significant changes. *[500 char]* *When making comparisons, ensure that you compare same-year-to-same-year (e.g., the FY16 level for 2016 versus the FY17 level for 2016).*

Section D: Acquisition/Contract Strategy

Existing Contracts

In the table below, provide all awarded prime contracts (or task orders) for the Investment (sub-award details are not required). Planned contracts/procurements in pre-award are not to be included. Completed contracts do not need to be included. Data definitions can be found at https://www.fpds.gov/fpdsng_cms/index.php/en/worksite.html.

For contract details like contract value and contract types, OMB will pull the authoritative data from FPDS.gov. If the Investment IPT has questions regarding the data pulled from FPDS, the IPT lead should contact the contract specialist on the IPT with questions.

Field	Data Description
Procurement Instrument Identifier (PIID)	The unique identifier for each contract, agreement, or order (FPDS data element 1A).
Referenced PIID	The unique identifier for the Indefinite Delivery Vehicles (IDV), such as a Government-wide Acquisition Contract (GWAC), Indefinite Delivery Contract, Federal Supply Schedule (FSS), Basic Ordering Agreement (BOA), or Blanket Purchase Agreement (BPA) under which the contractor support was obtained. This field is only required for IDVs and is FPDS data element 1C.
Modular Approaches/ Contracting	Information if acquisition planning, award, and management actions apply the principles and strategies described in "Contracting Guidance to Support Modular Development"? *[Yes/No]*
Agile Development	Does this contract employ agile development techniques? *[Yes/No]*
EVM Required?	*[Yes/No]*
Purpose of needing this procurement.	A brief description of the purpose of the award, the goods or services to be obtained under the award, and how they fit in the overall project. *While the description in FPDS could be used, OMB requests the Investment IPT provide a summary description for this field to supplement the FPDS data as the IPT information will provide more details.* *[500 char]*
IT Lease	If this acquisition/contract contains a lease (as defined by OMB Circular A-11 Appendix-B), what kind of lease does this contract include? Select from: • Lease-purchase without substantial private risk • Lease-purchase with substantial private risk • Capital lease • Operating lease • Other
Information Security Clause	Does this contract include information security clauses regarding the use, storage or other processing of data? *[Yes/No]*

Acquisition Strategy

For planned procurements for this Investment (including those in any pre-award phase, to include active solicitation) please provide the following table. Information on planned Intra-Agency Agreements (IAA) or Memoranda of Understanding (MOU) should be included in table 2 of this section.

Field	Data Description
Description of the planned contract support	A brief description of the planned purpose of contract or Inter-Agency support, the expected outcomes to be obtained, the support to be acquired (goods or services) and which project outcome or goal will be met or supported by this contract support. *[1000 char]*
Anticipated award date or	*[MM/DD/YYYY]*

IAA/MOU signature	
Length of planned period of support	What is the expected time frame for which this support is needed (please express in terms of base time frame and options? *[e.g. 90 days, 180 days, 1 year, 2 years, 5 years] [20 char]*
Anticipated Value	The anticipated value of the required support.
Modular Approaches/ Contracting	Does the acquisition planning, award, and management approach apply the principles and strategies described in "Contracting Guidance to Support Modular Development"? *[Yes/No]*
Will there be Agile Development	Does this contract or suite of contracts or IAA or MOU employ agile development techniques? *[Yes/No]*
Will EVM be Required?	*[Yes/No]*
Potential sources	What existing sources (schedules, BPAs, contracts, Inter-Agency collaborations, or other shared services) or shared services have been considered as potential solutions or sources to meet this need? *[CIOSP3, Schedule 70, etc.]* *[500 char]*
Provider engagement	What strategies are being considered to reach out to innovative provider has been performance? *[Market engagement, RFIs, industry days, etc.]* *[1000 char]*
IT Lease	Might this planned procurement contain a lease (as defined by OMB Circular A-11 Appendix-B)? *[Yes/No]* *Note*: Agencies are required to submit to their OMB representatives leasing and other non-routine financing proposals for review of the scoring impact and budget requirements (see A-11 Appendix B—Budgetary Treatment of Lease-Purchases and Leases of Capital Assets).

If the planned contract support or shared service replaces an existing contract arrangement, provide the existing contract(s) that this procurement will replace/restructure or supplement. For each existing contract provide the following:

Field	Data Description
PIID	The unique identifier for each contract, agreement, or order, (FPDS data element 1A)
Referenced PIID	The unique identifier for the Indefinite Delivery Vehicles (IDV), such as a Government-wide Acquisition Contract (GWAC), Indefinite Delivery Contract (IDC), Federal Supply Schedule (FSS), Basic Ordering Agreement (BOA), or Blanket Purchase Agreement (BPA) under which the contractor support was obtained This field is only required for IDVs. And is FPDS data element 1C

Section E: Systems Inventory (Administrative Services and Support Systems only)

For Investments designated as Part 2 - Administrative Services and Support Systems in column 6 (by entering code "02") of the IT Investment Portfolio Summary, provide a list of systems included in this Investment.

Note: Responses to this field are per FISMA definitions.

Field	Data Description
System Name	*[250 char]*
Initial Operating Year	*[YYYY]*
Last Major Tech Refresh Date	*[MM/DD/YYYY]*
End of Contracted Support	*[MM/DD/YYYY]*
Average # of users per month	*[10 digit integer]*

Section F: Costs and Capabilities (for IT Security and Compliance Standard Investment(s) only)

Cybersecurity is a top priority for the Administration, and Agencies are now required to report on their standard Investments for IT Security and Compliance at the level that it is managed and executed. In the spirit and support of FISMA and FITARA, every organization managing a security program must now report a business case to provide visibility of costs and outcomes of its cybersecurity activities. The intent is not a single, consolidated business case for IT Security and Compliance across the Agency, rather individual Investments reflecting the point at which they are managed.

Each dollar spent should maintain or enhance security posture and reduce risks. The intent of this business case is to align budget with performance measures that drive cybersecurity outcomes, an outcome which will be achieved using data provided in this business case in combination with Agency-reported FISMA metrics. Agencies have long reported their performance on metrics tied to the fulfillment of FISMA, which has allowed OMB to analyze performance over time. During the FY 2017 President's Budget Process, OMB began tying both FISMA metrics and Agency-reported spending on cybersecurity efforts to the NIST Cybersecurity Framework. Aligning these data collections allowed OMB to better understand how Agencies were distributing their cybersecurity resources and compare these results to Agency performance on the associated FISMA metrics. The IT Security and Compliance Investment Business Case will further this effort, allowing even greater understanding of how Agency and bureau budgeting behavior is driving cybersecurity performance in key areas. Tables A and B provide Agencies and bureaus with the ability to report cyber spending at the sub-component/tool level. OMB understands the need for maximum Agency flexibility in budgeting for cybersecurity and urges Agencies to use this business case as a tool to clearly explain the value derived from bureau-level and Agency-wide Investments in IT Security and Compliance.

Each record in the table below should represent a unique security capability that corresponds to a NIST Framework Category (see http://www.nist.gov/cyberframework/). The total spending for a given category will be aggregated based on the spending reported under the capabilities for that category. If no capabilities are reported for a NIST Framework Category, there will be zero spending associated with that category.

For any Investment designated as an IT Security and Compliance Standard Investment (code "02" in Column 7 of the IT Investment Portfolio Summary), complete the following table:

Column	Description
1	**NIST Framework Category** Each capability will be mapped to one of the 5 categories below: 1) Identify 2) Protect 3) Detect

	4) Respond 5) Recover
2	**Capability** List the capability associated with the spending in the PY, CY and/or BY years. Agencies are not required to submit a record for each capability or NIST Framework Category; however, at the Agency level, Agencies should try to ensure they provide at least one Capability for each NIST Framework Category. To facilitate more complete reporting, each NIST Framework Category includes an *Other* capability category Agencies may utilize for cybersecurity costs that would not have otherwise been accounted for. Agency spending in any specific *Other* capability category should not exceed $10 million. If the reported spending exceeds $10 million, Agencies should break the Investment into smaller, individual components and describe them in greater detail. The descriptions of each capability are included in Appendix D.
3	**Purpose/Outcome** Describe the purpose and intended outcomes from money spent on the reported capability. Also describe any expected fluctuations in spending across the 3 years. *[1000 char]*
4	**Budget Account** Enter the OMB budget account or accounts funding each capability.
5	**PY 2016 Total** Indicate the total PY 2016 spending on the reported capability.
6	**CY 2017 Total** Indicate the total CY 2017 planned spending on the reported capability.
7	**BY 2018 Total** Indicate the total BY 2018 planned spending on the reported capability.

MAJOR IT BUSINESS CASE DETAIL

Major IT Business Case Detail is used to provide OMB with Current Year (FY 2017) and Budget Year (FY 2018) Investment plans and performance data. Include in this exhibit, at a minimum, all projects, activities, and operations scheduled to commence or continue in the CY and/or BY. Information in the Major IT Business Case Detail should reflect current status; therefore, the Federal ITDB should be updated as soon as the data becomes available for continuous updates.

In Major IT Business Case Detail, Investments are described as:

- Investment
  - Projects
    - Activities
  - Operations

Report information about these areas in the following Major IT Business Case Detail sections:

A.1: ***General Information***: Enter basic information about the major IT Investment.
A.2: ***Investment Risk:*** Identify all open risks to the Investment.
B.1: ***Projects****:* Identify all of the Investment's projects with activities occurring in CY and BY.
B.2***: Activities****:* Outline the activities that are performed to achieve the outcome of each project.
C.1: ***Operational Performance Information****:* Identify performance targets and results for evaluating operations.

Section A.1: General Information	
Column /Field	**Description**
1	**Investment Name** Agency-provided name of Investment, consistent with Agency IT Portfolio Summary.
2	**Investment UII** Agency-provided UII, consistent with Agency IT Portfolio Summary.

Section A.2: Investment Risk

Risk assessments should include both project and operational risk information from all stakeholders and should be performed throughout the life cycle of the Investment. This sections should follow the Regular Updates Reporting schedule (see Section 2.3).

In Table A.2, list active risks at the Investment level and provide risk assessment information. The risks listed should be consistent with what is included in management briefings or Agency status reviews on an ongoing basis. It is not necessary to address all 19 OMB Risk Categories. There are not a specified number of risks for Agencies to include for each Investment. Include the following data in Table A.2:

Column /Field	Description
1	**Risk Name** A short description that identifies the risk, the cause of the risk and the effect that the risk may have on the Investment. *[500 char]*
2	**Risk Category** The relevant OMB Risk Category for each risk. Risk categories include: 1) Schedule 2) Initial costs 3) Life cycle costs 4) Technical obsolescence 5) Feasibility

	6) Reliability of systems 7) Dependencies and interoperability between this Investment and others 8) Surety (asset protection) considerations 9) Risk of creating a monopoly for future procurements 10) Capability of Agency to manage the Investment 11) Overall risk of Investment failure 12) Organizational and change management 13) Business 14) Data/info 15) Technology 16) Strategic 17) Security 18) Privacy 19) Project resources
3	**Risk Probability** The likelihood of a negative impact for the risk. *[Low, Medium, High]*
4	**Risk Impact** The level of a potential negative impact for the risk. *[Low, Medium, High]*
5	**Mitigation Plan** A short description of how to mitigate the risk. *[500 char]*

Section B: Project Plan and Execution Data

Tables B.1, B.2.1, and B.2.2 are used to report all projects with activities underway in any portion of CY or BY, regardless of where the project occurs in the Investment life cycle (projects may be conducted in Planning, DME, and/or Maintenance). At a minimum, Tables B.1, B.2.1 and B.2.2 should include:

- Projects and activities that started in a previous fiscal year (PY and earlier) that have not been completed by the beginning of the CY; and
- Projects and activities that start and finish in the CY and BY **or** start but do not finish in CY or BY.

If the Investment/program uses an automated tool for requirements gathering, tracking, planning, or management, identify the automated tool. Projects and activities commencing beyond the BY may also be reported, as available.

Include the following data in Table B.1:

Column /Field	Description
1	**Unique Project ID** An Agency-specified number that uniquely identifies the project within the Investment.
2	**Project Name** Name used by the Agency to refer specifically to the project.
3	**Objectives/Expected Outcomes** Description of the project's functionality, capability, or goal.
4	**Project Start Date** Actual start date of in-progress projects or planned start of projects that have not yet begun (may be before the current FY or activities listed in Table B.2.1). *[MM/DD/YYYY]*
5	**Project Completion Date** Planned date of completion of in-progress projects or actual completion date of projects that have been completed (may be after BY or completion date of activities listed in activities Table B.2.1). *[MM/DD/YYYY]*
6	**Project Life-Cycle Cost** Enter the total cost of all activities related to the project as described in OMB Circular A-131 (in $ millions). This only includes costs for the project, and does not include O&M or other

Column /Field	Description
	sustainment costs.
7	**System Development Life Cycle (SDLC) Methodology** Which development methodology does this project use? 1) Waterfall 2) Spiral 3) Iterative (Prototyping/Incremental) 4) Agile 5) Mixed 6) Other 7) Not Primarily a Software Development Project
8	**Other SDLC?** If you selected "Other" provide the name of the SDLC methodology this Project is using.
9	**Production Release every 6 months** Does this Project have a production release containing useable functionality at least every 6 months? *[Yes, No, N/A]*
10	**Comment** If this Project does not provide a production release at least every 6 months, please provide a rationale as to why.
11	**When was the last date that a revised product was deployed to production?** This question collects information on how frequently changes to the system are deployed. A change can mean a new or removed feature, a patch, or a bug fix that was deployed via a change in the system's application code. If a system is under version control, this date can be easily determined by looking at the date on which the most recent commit to the production version of the codebase was made. If there has not yet been a release to production, provide the projected first production deployment date. This field is not required for SDLC Methodology 7 "Not Primarily a Software Development Project." [*MM/DD/YYYY]*

Each project listed in table B.1 should have at least one associated activity. Please include any relevant non-agile project activities in Table B.2.1 and include agile project activities in Table B.2.2.

Project Activity Table B.2.1

In Table B.2.1, describe, at a minimum, all non-agile project activities for projects in Table B.1 that started in a previous FY (PY and earlier) and that have not been completed by the beginning of the CY, as well as activities that are scheduled to start in the current FY and BY. In line with modular development principles, each software development project must produce usable functionality at intervals of no more than six (6) months. Include the following data in Table B.2.1:

Column /Field	Description
1	**Unique Project ID** An Agency-specified number that uniquely identifies the project within this Investment.
2	**Activity Name** A short description consistent with the critical steps within the Agency project management methodology.
3	**Activity Description** Describe what work is accomplished by the activity.
4	**Structure ID** Agency-specified identifier that indicates the work breakdown structure (WBS) the Agency uses to associate the activity with other activities or a project. Provide this in the format of "x.x.x.x.x" where the first string is the Unique Project ID and each following string (separated by periods) matches the structure ID of a parent activity. See below for more guidance about parent and child activities expressed through this structure. *[x.x.x.x.x]*
5	**Type of Activity** This should only be provided for activities that do not have a child (i.e., lowest level) and that are active/open as of October 1, 2015. Not every project will have every type of activity listed

Column /Field	Description
	below. Completion of this activity primarily provides: 1) Conceptualization/Planning 2) Requirements Gathering 3) Design / User Experience (UX) 4) Prototype 5) Development 6) Security Testing 7) Iterative Testing 8) Iterative Release 9) Regression Testing 10) User Acceptance Testing 11) Development Operations (DevOps) / Configuration Management 12) Quality Assurance 13) Production Release 14) Retirement 15) This is not a software development related activity 16) Other
6	**Critical Path** Is this activity on the critical path of the successful completion of the project. *[Yes/No]*
7	**Start Date Planned** The planned start date for the activity. This is the baseline value.
8	**Start Date Projected** If the activity has not yet started, enter the current planned start date of the activity.
9	**Start Date Actual** When the activity starts, enter the actual start date here.
10	**Completion Date Planned** The planned completion date for the activity. This is the baseline value.
11	**Completion Date Projected** If the activity has not yet completed, enter the current planned completion date of the activity.
12	**Completion Date Actual** When the activity ends, enter the actual completion date here.
13	**Total Costs Planned** The planned total cost for the activity. This is the baseline value. *[$M]* *Note*: For programs that are employing earned value management, Agencies should reflect "budget at completion" in the "Total Costs Planned" field and "estimated at completion" in the "Total Costs Projected" field.
14	**Total Costs Projected** When the activity is not yet completed, enter the current planned total cost of the activity. *[$M]* *Note*: For programs that are employing earned value management, Agencies should reflect "budget at completion" in the "Total Costs Planned" field and "estimated at completion" in the "Total Costs Projected" field.
15	**Total Costs Actual** When the activity ends, enter the actual total costs for the activity here. *[$M]*

Reporting Parent and Child Activities (WBS Structure)

"Child" activities may be grouped under "Parent" activities to reflect the WBS used by the Agency to manage the Investment. If a WBS is not used by the Agency, report the relationship between parent activities and child activities in "Structure ID" using this method. Agencies are encouraged to report a transparent view of the Investment baseline on the Federal ITDB (at least Level 3 of the WBS). Levels 1 and 2 typically do not provide enough information to describe the work to be accomplished in short enough duration that early warnings of Investment performance can be identified (M-10-27).

When reporting an activity, enter the "Structure ID" as a period-delimited string consisting of the "Unique Project ID" and each nested parent activity between the project level and the child activity. The "Structure ID" to enter will vary depending on the activity's WBS level.

Example: For child activity 3 that is part of parent activity 10, which in turn is part of parent activity 2, which in turn is part of Project A, enter: A.2.10.3

- Project A
  - Parent Activity 2
    - Parent Activity 10
      - Child Activity 3

There is no limit to the number of nested "child" and "parent" relationships allowed, and this depth may vary from activity to activity and from project to project.

If any of a parent activity's child activities occurs in the current FY, then all child activities of the parent activity must be reported, regardless of their timing. This is to ensure that a complete view of the parent activity is available.

All activities with no child activities must have, at a minimum*, Unique Project ID, Activity Name, Activity Description, Structure ID, Type of Activity, Start Date Planned, Start Date Projected (or Actual), Completion Date Planned, Completion Date Projected (or Actual), Total Costs Planned,* and *Total Costs Projected (or Actual)*.

Completed activities must also have *Start Date Actual, Completion Date Actual,* and *Total Costs Actual*. Any parent activities with a child activity must be completely described by the aggregate attributes of its child activities. In the ITDB, the cost and schedule information for parent activities will be based on the cost and schedule information of the lowest level of child activities reported. Agency-submitted cost and schedule information is not required for parent activities.

Unique Project ID	Activity Name	Structure ID	Start Date Planned	Completion Date Planned	Planned Total Costs	…
A	*Design*	*A.2*	*2/1/2015*	*2/29/2015*	*$2.5*	
A	Business Requirements	A.2.1	2/1/2015	2/10/2015	$1.0	
A	Technical Requirements	A.2.2	2/11/2015	2/20/2015	$1.0	
A	Architecture	A.2.3	2/21/2015	2/29/2015	$0.5	

Parent activities like the one highlighted above (Structure ID: A.2) are optional. Reported parent activities values will be ignored, as calculated values will be determined by aggregating the cost and schedule information reported in the child activities.

Project Activity Table B.2.2

If agile methodology is being used, the below table can be leveraged as an alternative to Table B.2.1. This table is being added as an optional alternative to table B.2.1 for agile-based development projects. It is consistent with OMB's forthcoming agile guidance and comes at Agencies' request for an agile-friendly alternative to report performance. Either table B.2.1 or B.2.2 should be used to enter project activity data; the same project should not appear in both tables. In Table B.2.2, describe, at a minimum, all agile project activities for projects in Table B.1 that started in a previous FY (PY and earlier) and that have not been completed by the beginning of the CY, as well as activities that are scheduled to start in the current FY and BY. The terms and concepts in Table B.2.2 are based on the Agile Scrum Methodology. If you are using another agile methodology, still complete the table in line with the Agile Scrum Methodology.

Column /Field	Description
1	**Unique Project ID** An Agency-specified number that uniquely identifies the project within this Investment.
2	**Release Name** (Activity Name) Feature as defined in Product Backlog.
3	**Release Number** Iteration/Feature as defined in Product Backlog.
4	**Release Description** (Activity Description)
5	**Start Date Planned** Release start date planned. *[MM/DD/YYYY]*
6	**Start Date Projected** Release start date projected. *[MM/DD/YYYY]*
7	**Start Date Actual** Release start date actual. *[MM/DD/YYYY]*
8	**Completion Date Planned** Release completion date planned. *[MM/DD/YYYY]*
9	**Completion Date Projected** Release completion date projected. *[MM/DD/YYYY]*
10	**Completion Date Actual** Release completion date actual. *[MM/DD/YYYY]*
11	**Total Costs Planned** Total cost planned for the release. *[$M]*
12	**Total Costs Projected** Total cost projected for the release. *[$M]*
13	**Total Costs Actual** Total cost actual for the release. *[$M]*
14	**NPI** Number of planned iterations/sprints in the release.
15	**NPE** Number of planned Epics (fraction of an Epic is acceptable).
16	**NCE** Number of completed Epics in a release (fraction of an Epic is acceptable).
17	**NCI** Number of completed iterations/sprints in a release.
18	**DTC** How many direct technical contributors are on the project (inclusive of government or contractor engineers and designers that contribute directly to the code base; this number might not equate to the total FTE at the Investment level).
19	**DPC** How many other staff contribute directly to the project (inclusive of government or contractor project managers, testers, agile coaches, and others; this number might not equate to the total FTE at the Investment level).

Section C: Operational Data

Section C applies to operational and mixed life-cycle Investments with operational components. It focuses on operational analysis results and performance metrics.

Operational Analysis

Provide the date and results of the last Operational Analysis (for operational and mixed life cycle systems/Investments).

Date of Analysis	Analysis Results
[MM/DD/YYYY]	*[Limit: 2500 char]*

Operational Performance
Ongoing performance of operational Investments is monitored to demonstrate the existing Investment is meeting the needs of the Agency, delivering expected value, and/or that the modernized and replaced systems are consistent with the Agency's enterprise architecture. Measures should be as "outcome" based as possible rather than "output" based and should help the Investment benchmark its relative performance. Performance measures are used in the operational analysis and alternatives analysis to compar e possible alternatives and can also be used to validate the need for future Investment. The OMB Capital Programming Guide (page 44) directs that operational performance metrics should seek to answer more subjective questions in the specific areas of:

- Customer Satisfaction (Results);
- Strategic and Business Results;
- Financial Performance; and
- Innovation

Customer Satisfaction (Results) – Metrics should focus on whether the Investment supports customer (internal and/or external) processes as designed. The focus is on how well the Investment is delivering exceptional customer services.

Strategic and Business Results – Metrics should measure the effectiveness and the efficiency of the Investment in meeting its Agency's mission, strategic objectives and or priority goals, as well as its technical ability to deliver at the level of quality and reliability needed by the customer/end user.

Financial Performance – Metrics should compare current performance with a pre-established cost baseline. While financial performance is typically expressed as a quantitative measure, the Investment should also be subjected to a periodic review for reasonableness and cost efficiency. This type of measure is often referred to as "cost per unit" measures. Possible examples include cost per transaction, cost per mailbox, cost per user, or cost per query, etc. Financial Performance measures are used in the Operational analysis and Alternatives analysis to compare possible alternatives and can also be used to validate the need for future Investment.

Innovation – Metrics should focus on true Research and Development (R&D) or prototyping activities. A possible example of a performance metric in the innovation category would be "number of new ideas per employee".

A minimum of five (5) metrics must be reported, across three (3) areas:

1. ***Customer Satisfaction (Results):*** Provide a minimum of one (1) metric that reflects results (i.e. service quality, end user satisfaction) with respect to the impact to major stakeholders (customers, affected citizens, inter and Intra-Agency end users).
2. ***Strategic and Business Results:*** Provide a minimum of three (3) metrics that measure how this Investment contributes to the Strategic Objectives/Agency Priority Goals or business need of the Agency. These could come in two different areas. At least one Strategic and Business Results metric must have a monthly reporting frequency.
    a. ***Effectiveness*** **–**quantified desired effect the Investment has on the Agency's mission or business needs (e.g. processing speed, processing quality, backlog reduction, mission outcomes, business outcomes, etc.)

   b. ***Efficiency -*** quantified desired effect the Investment has on the Agency's operational/technical needs (e.g. reliability, availability, throughput, response time/latency, utilization, etc.)
3. ***Financial Performance:*** Provide a minimum of one (1) metric that measures the reasonableness and cost efficiency of the Investment.
4. ***Innovation:*** Investments are not required to report innovation metrics for every Investment, however Agencies may choose to report under Innovation metrics category if they so choose. (M-14-11)

All data will be displayed to the public on the ITDB. Ensure that all metrics provided are publicly releasable.

Defining Metrics

Use the following table to define the attributes of each individual metric:

Table C.1.A	
Column /Field	**Description**
1	**Metric ID** Unique ID provided by Agency for the metric. When reporting actual results (see below), use this ID to reference the correct metric. *[numeric]*
2	**Metric Description** Description to help the user understand what is being measured. In this field, describe the units used, any calculation algorithm used, and the definition or limits of the population or "universe" measured. *[500 char]*
3	**Unit of Measure** Brief indication of what quantity is measured (e.g. number, percentage, dollar value) for each metric. *[50 char]*
4	**Performance Measurement Category Mapping** Identify the measurement category, as shown above table C.1A. *[Measurement Category]*
5	**Agency Baseline Capability** What was the quantitative value of your Agency's capability per this metric prior to this Investment's life cycle. If your Agency has not measured this capability before, you may leave this field blank; otherwise, provide the numeric value of the historic capability measurement.
6	**2016 Target** Metric target value from 2016, relative to the reporting frequency. *[numeric]*
7	**2017 Target** Metric target value for 2017, relative to the reporting frequency. *[numeric]*
8	**Measurement Condition** Indicates whether a desired result would be "over target," indicating that the trend should maintain or increase, or "under target," indicating that the trend should maintain or decrease. *[Over target/Under target]*
9	**Reporting Frequency** How often actual measurements will be reported (monthly, quarterly, semi-annually, or annually). Annual reporting frequencies are reserved for annual operating cost measures, performance measures associated with the Agency's annual performance plan, or other measures that can only be appropriately measured on an annual basis. *[Monthly, Quarterly, Semi-Annual, Annual]*
10	**Agency Strategic Objective or Priority Goal** Each Investment must have at least one active metric in the Strategic and Business Results category (of any reporting frequency) tied to the foremost Agency strategic objective (SO), or Agency priority goal (APG) (as required by A-11 Section 230 and Section 250 respectively). Provide that code for the associated metric, using the appropriate code on performance.gov). Agencies that are not required to report to performance.gov may use the "0" code. *[Goal Code]*
11	**Is the Metric Retired?**

Table C.1.A	
Column /Field	**Description**
	Check this box when performance metrics are no longer useful for Investment management. *[Check Box]*

Providing actual results

As actual results are measured at the appropriate frequency, they should be reported as new entries in Table C.1B:

Table C.1.B	
Column /Field	**Description**
1	**Metric ID** Unique ID provided by Agency for the metric. When reporting actual results (see below), use this ID to reference the correct metric. *[numeric]*
2	**Actual Result** Actual result measured. *[numeric]*
3	**Date of Actual Result** End date of the most recent reporting period. *[MM/DD/YYYY]*
4	**Comment** Comments for metrics that have not been met will be valuable for OMB and Agency Reviewers. *[500 char] (optional)*

When adding a new metric, include historical actual result information as available.

Appendix A. Legal Regulatory Authorities

The Federal Government must effectively manage its portfolio of capital assets to ensure scarce public resources are wisely invested. Capital programming integrates the planning, acquisition, and management of capital assets into the Budget decision-making process. It is intended to assist Agencies in improving asset management and in complying with the results-oriented requirements of:

- The Federal Information Technology Acquisition Reform (FITARA) is Title VIII Subtitle D Sections 831-837 of H.R.3979 - Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 available at https://www.congress.gov/bill/113th-congress/house-bill/3979/text (P.L. 113-291).

- The Clinger-Cohen Act of 1996, which requires Agencies to use a disciplined CPIC process to acquire, use, maintain, and dispose of IT in alignment with the Agency's EA planning processes. OMB policy for the management of Federal information resources is detailed in Circular No. A-130 (P.L. 104-106), Management of Federal Information Resources.

- The Government Performance and Results Act (GPRA) of 1993, which establishes the foundation for Budget decision making to achieve strategic objectives in order to meet Agency mission objectives. Instructions for preparing strategic plans, annual performance plans, and annual program performance reports are provided in Part 6 of OMB Circular No. A-11, Section 220 (P.L. 103-62).

- The GPRA Modernization Act of 2010 (P.L. 111-352), which requires quarterly performance assessments of Federal Government priorities and establishes Agency Performance Improvement Officers and the Performance Improvement Council.

- The Federal Managers Financial Integrity Act of 1982 (P.L. 97-255), Chief Financial Officers Act of 1990 (CFO Act) (P.L. 101-576), and Federal Financial Management Improvement Act of 1996 (P.L. 104-208), which require accountability of financial and program managers for financial results of actions taken, control over the Federal Government's financial resources, and protection of Federal assets. OMB policies and standards for developing, operating, evaluating, and reporting on financial management systems are contained in Circular No. A–127, Financial Management Systems and OMB Circular No. A-11, Section 52.

- The Paperwork Reduction Act of 1995 (P.L. 96-511), which requires Agencies to perform their information resources management activities in an efficient, effective, and economical manner.

- The Federal Information Security Management Act (FISMA) of 2002 (P.L. 107-347), which requires Agencies to integrate IT security into their capital planning and EA processes, conduct annual IT security reviews of all programs and systems, and report the results of those reviews to OMB.

- The E-Government Act of 2002 (P.L. 107–347), which requires Agencies to support Government-wide E-Government (E-Gov) initiatives and to leverage cross-Agency opportunities to further E-Gov. The Act also requires Agencies to establish a process for determining which government information the Agency intends to make available and accessible to the public on the Internet and by other means. In addition, the Act requires Agencies to conduct and make publicly available privacy impact assessments (PIAs) for all new IT Investments, administering information in an identifiable form collected from or about members of the public.

- The National Technology Transfer and Advancement Act of 1995 (P.L. 104-113) and OMB Circular No. A-119, which state that voluntary consensus standards are the preferred type of standards for Federal Government use. When it would be inconsistent with law or otherwise impractical to use a voluntary consensus standard, Agencies must submit a report to OMB through NIST describing the reason(s) for the Agency's use of government-unique standards in lieu of voluntary consensus standards.

- The Federal Records Act (44 U.S.C. Chapters 21, 29, 31, and 33), which requires Agencies to establish standards and procedures to ensure efficient and effective records management. The National Archives and Records Administration (NARA) issues policies and guidance for Agencies to meet their records management goals and requirements. NARA also provides policies and guidance for planning and evaluating Investments in electronic records management.

- The Privacy Act of 1974 (5 U.S.C. § 552a), which is an omnibus "code of fair information practices" that attempts to regulate the collection, maintenance, use, and dissemination of personal information by Federal executive branch Agencies.

- NIST Special Publication 800-146 concepts and definitions regarding cloud computing.

- Recent OMB IT policies and guidance, including:
  - Federal Information Technology Shared Services Strategy
  - The Common Approach to Federal Enterprise Architecture
  - Contracting Guidance to Support Modular Development
  - The Federal Cloud Computing Strategy
  - Digital Government Strategy: Building a 21st Century Platform to Better Serve the American People
  - Security Authorization of Information Systems in Cloud Computing Environments (FedRAMP)
  - National Strategy for Information Sharing and Safeguarding
  - OMB memo M-11-29 – Chief Information Officer Authorities
  - OMB memo M-13-08 – Improving Financial Systems Through Shared Services
  - OMB memo M-13-09 – Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management
  - OMB memo M-13-13 – Open Data Policy-Managing Information as an Asset
  - OMB memo M-13-14 – Fiscal Year 2016 Budget Guidance
  - OMB memo M-14-03 – Enhancing the Security of Federal Information and Information Systems
  - OMB memo M-14-08 – Fiscal Year 2015 PortfolioStat
  - OMB memo M-15-14 – Management and Oversight of Federal Information Technology
  - OMB memo M-16-11 – Improving Administrative Functions Through Shared Services

- Executive Order 13514, Federal Leadership in Environmental, Energy, and Economic Performance

- Executive Order 13423, Strengthening Federal Environmental, Energy, and Transportation Management
- Executive Order 13642, Making Open and Machine Readable the New Default for Government Information, May 9, 2013
- Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information
- Federal Acquisition Regulation, including subchapter B, parts 5 through 12 and part 23
- Federal Management Regulation, including subchapters B and C
- Energy Independence and Security Act of 2007 (P.L. 110-140), including sections 431 through 435 and 523 through 525
- Energy and Policy Act of 2005 (P.L. 109–58), including sections 103, 104, 109, and 203

Appendix B. Coding Instructions for Shared Services Investments

For Agencies' shared services Investments which are not included in the two tables below, these should be coded "48" for the "Shared Services Category" field in the IT Portfolio Summary.

E-Gov and LoB Initiative Investments (Shared Services Category Code "24")				
E-Gov or LoB Initiative	**Acronym**	**Managing Partner Agency**	**Includes**	**Shared Services Identifier**
Benefits.Gov		Labor		0020
Budget Formulation and Execution LoB	BFELoB	Education		3200
Disaster Assistance Improvement Plan		DHS		4100
E-Rulemaking		EPA		0060
Federal Health Architecture LoB	FHALoB	HHS		1400
Financial Management LoB	FMLoB	Treasury	Former GMLoB	1100
Geospatial LoB	GeoLoB	Interior		3100
Grants.Gov		HHS		0160
Human Resources LoB	HRLoB	OPM		1200
Integrated Award Environment	IAE	GSA	Former IAE-Loans & Grants	0230
Performance Management LoB	PMLoB	GSA		0900
Federal PKI Bridge	FPKI	GSA		0090
Recreation.Gov		USDA		0010
Security, Suitability, and Credentialing LoB	SSCLoB	OPM	New UII ending assigned for FY17 process.	1250
USAJOBS	USAJOBS	OPM	Former RecruitOnestop	1218
USA Services		GSA		0040

OMB M-16-11 defined shared service providers as providers designated by Treasury FIT or OPM HRLOB previously and USSM going forward. The below table reflects current USSM designated shared services.

A Partner Agency should list its Investment as Type 04 Funding Transfer and report funding in the Agency Funding fields. Managing Partner Agency should report their Investment as a Type 01 Major Investment and reports funding from customers in the Agency Contribution fields.

USSM Designated Shared Services Investments/Providers (Shared Services Category Code "36")					
Shared Service Investment	**USSM Designated Shared Service Provider**		**Acronym**	**Includes**	**Shared Services Identifier**
Agency Accounting Services (AAS)	Treasury	Administrative Resource Center	ARC	Financial Management	1101
HR LoB - HR Connect	Treasury	Treasury Shared Service Center	TSSC	Core HR	1201
Defense Civilian Personnel Data System	DoD	Defense Civilian Personnel Advisory Service	DCPAS	Core HR	1202
Defense Civilian Pay System	DoD	Defense Finance and Accounting Service	DFAS	Payroll	1203
IBC FMLoB Shared Service Provider	DOI	Interior Business Center	IBC	Financial Management	1102
IBC Shared Service Center (HRLoB)	DOI	Interior Business Center	IBC	Core HR, Payroll	1204
DOTXX129: Delphi Version Two	DOT	Enterprise Services Center	ESC	Financial Management	1103
HHS Integrated Personnel Management Service	HHS	Program Support Center	PSC	Core HR	1205
Human Capital Information Technology Services	GSA	HRLoB Shared Service Center	HRLoB SSC	Core HR	1206
PAR (e-Payroll)	GSA	HRLoB Shared Service Center	HRLoB SSC	Payroll	1207
OCFO FSSP	USDA	National Finance Center	NFC	Financial Management	005-999991104
OCFO-NFC Shared Services	USDA	National Finance Center	NFC	Core HR, Payroll	005-999991208

Appendix C: Definitions

The list of common IT Budget – Capital Planning definitions is provided below:

Term	Source Document	Definition
Adequate Incremental Development	OMB Memo M-15-14 https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf	For development of software or services, planned and actual delivery of new or modified technical functionality to users occurs at least every six (6) months.
Agency Chief Information Officer (CIO), as defined in statute	OMB Memo M-15-14 https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf	The CIO at the headquarters level of a department or establishment of the government as defined in Section 20 of OMB Circular A-11 (contrasts with "Bureau CIO").
Agile Development	Forthcoming Agile Development Guidance	Means a development methodology that delivers functional software in shorter time iterations, from a couple of weeks to a couple of months. This is done through continuous planning, frequent reassessment and adaptation of plans, continuous testing , and continuous integration. A key component of agile is quick validation, emphasizing testing early and often with potential adopters of the software to ensure that the product works for its intended users. Agile development is used to describe any development process that is aligned with the concepts of the Agile Manifesto (https://www.agilemanifesto.org/principles.html).).
Alternatives Analysis	Capital Programming Guide	This term refers to a method for addressing the various options for meeting the performance objectives of an Investment, including the return on Investment of the various options. The analysis is performed prior to the initial decision to implement a solution and updated periodically, as appropriate, to capture changes in the context for an Investment decision. Alternatives Analysis should be performed for Investments with projects in the planning or DME stages, whereas strictly operational Investments should instead perform operational analyses until such time as a decision is made to re-evaluate the Investment or to resume development, modernization or enhancement. This terms refers to best practices outlined in the Capital Programming Guide under "I.4-Alternatives to Capital Assets" and "Evaluate Asset Options" (http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/capital_programming_guide.pdf).
Application Programming Interface (API)	IT Budget - Capital Planning Guidance	API refers to a protocol intended to be used as an interface by software components to communicate with each other. An API is a library that may include specification for routines, data structures, object classes, and variables.

Term	Source Document	Definition
Apportionment	31 U.S.C. § 1513(b); Executive Order 11541; OMB Circular A-11 Section 120	This term refers to an OMB-approved plan to use budgetary resources (31 U.S.C. § 1513(b); Executive Order 11541). It typically limits the obligations you may incur for specified time periods, programs, activities, projects, objects, or any combination thereof. It may also place limitations on the use of other resources, such as FTEs or property. An apportionment is legally binding, and obligations and expenditures (disbursements) that exceed an apportionment are a violation of, and are subject to reporting under, the Antideficiency Act (31 U.S.C. § 1517(a)(1), (b)).
Baseline	OMB Memo M-10-27	This term refers to the approved work breakdown structure, costs, schedule, and performance goals for a given Investment. For additional information on baselines and baseline management, see OMB Memo M-10-27, "Information Technology Investment Baseline Management Policy".
Benefit-Cost Analysis (BCA)	OMB Circular A-94; Capital Planning Guide	Benefit-Cost Analysis refers to the recommended technique to use in a formal economic analysis of government programs or projects. Guidance for Benefit-Cost Analysis is described in OMB Circular A-94.
Budget Authority	OMB Circular A-11 Section 20.4	Authority provided by federal law to enter into financial obligations that will result in immediate or future outlays involving Federal Government funds. The basic forms of budget authority include (1) appropriations, (2) borrowing authority, (3) contract authority, and (4) authority to obligate and expend offsetting receipts and collections.
Budgetary Resource	OMB Circular A-11 Section 20.4	This term refers to an amount available to enter into new obligations and to liquidate them. Budgetary resources are made up of new budget authority (including direct spending authority provided in existing statute and obligation limitations) and unobligated balances of budget authority provided in previous years. Direct spending authorities include appropriations and collections of fees authorized under 42 U.S.C. § 14953.
Bureau CIO	OMB Memo M-15-14 https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf	Official with the title or role of CIO within a principal subordinate organizational unit of the Agency, as defined in Section 20 of OMB Circular A-11, or any component organization of the Agency (contrasts with "Agency CIO").
Business Reference Model (BRM)	FEA Consolidated Reference Model Document, Version 2.3	This term refers to one of six (6) reference models of the Federal Enterprise Architecture. The BRM is a classification taxonomy used to describe mission sectors, business functions, and services that are performed within and between Federal Agencies and with external partners. It provides a functional view of Federal Government organizations and their LoBs, including mission and support business services opportunities for collaboration, shared services, and solution reuse can be identified by mapping IT Investments to the BRM.
Capital Assets	Appendix one of the Capital Programming Guide	Capital Assets refer to land, structures, equipment, intellectual property (e.g., software), and IT (including the output of IT service contracts) that has been acquired

Term	Source Document	Definition
		by the Federal Government and have an estimated useful life of two years or more. See Appendix One (1) of the Capital Programming Guide for a more complete definition of capital assets.
Capital Investment (or Investment)	IT Budget - Capital Planning Guidance	This term refers to the planning, development, and acquisition of a capital asset and the management and operation of that asset through its usable life after the initial acquisition. IT capital Investments may consist of one or more assets which provide functionality in an operational (production) environment.
Capital Planning and Investment Control (CPIC)	40 U.S.C. § 11302	This term refers to a decision-making process that ensures IT Investments integrate strategic planning, budgeting, procurement, and management of IT in support of Agency missions and business needs. The CPIC process has three distinct phases: Select, Control, and Evaluate. See 40 U.S.C. § 11302 for statutory requirements and Clinger-Cohen Act of 1996.
Capital Programming	IT Budget - Capital Planning Guidance	This term refers to an integrated process within an Agency that focuses on the planning, budgeting, procurement, and management of the Agency's portfolio of capital Investments to achieve the Agency's strategic goals and objectives with the lowest overall cost and least risk.
Cloud Computing	NIST Special Publication 800-145 -The NIST Definition of Cloud Computing	Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing promotes availability and is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service); three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and, four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud). Key enabling technologies include: (1) fast wide-area networks, (2) powerful, inexpensive server computers, and (3) high-performance virtualization for commodity hardware (see NIST Special Publication 800-145 -The NIST Definition of Cloud Computing http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf for official government definition).
Cloud Computing Spending	IT Budget - Capital Planning Guidance	This term refers to implementation and operational costs directly attributable to the cloud computing systems within the Investment for the specified year.
Cloud First Policy	OMB Memo M-13-09	This term refers to OMB's Cloud First policy, launched in December 2010, which is intended to accelerate the pace at which the government realizes the value of cloud computing by requiring Agencies to evaluate safe, secure cloud computing options before making any new Investments. Per the Federal Cloud Computing Strategy,

Term	Source Document	Definition
		Agencies should evaluate their technology sourcing plans to include consideration and application of cloud computing solutions as part of the budget process. Agencies should seek to optimize the use of cloud technologies in their IT portfolios to take full advantage of the benefits of cloud computing in order to maximize capacity utilization, improve IT flexibility and responsiveness, and minimize costs. When evaluating options for new IT deployments, OMB requires that Agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. Additionally, Agencies shall continually evaluate cloud computing solutions across their IT portfolios, regardless of Investment type or life cycle stage. http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf - Page 2 and http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-09.pdf
Collaboration Tools	FEA Consolidated Reference Model Document, Version 2.3	Collaboration tools include all software and services used to support digital collaboration (e.g., wiki, social media services, document/file sharing, web conferencing solutions, and text messaging, desktop video conferencing solutions). Capabilities that allow for the concurrent, simultaneous communication and sharing of content, schedules, messages and ideas within an organization: Threaded Discussions support the running log of remarks and opinions about a given topic or subject; Document Library supports the grouping and archiving of files and records on a server; Shared Calendaring allows an entire team as well as individuals to view, add and modify each other's schedules, meetings and activities; Task Management supports a specific undertaking or function assigned to an employee. • Costs include all IT related to the collaboration solution including software licenses, server, communications, and specialized hardware equipment, data center allocation / charges, storage, backup solution, and contractors. • Does NOT include IT costs related to e-mail, office productivity software (e.g., office software suites, groupware, e-mail clients), or services for which the Agency does not pay (e.g., OMB MAX). • Does NOT include IT costs associated with conference-room audio or video teleconferencing as these are included under telecommunications.
Commodity IT	OMB Memo M-11-29, OMB Memo M-12-10, Federal IT Shared Services Strategy	This term refers to a category of back-office IT services whose functionality applies to most, if not all, Agencies (e.g., infrastructure and asset management, e-mail, hardware and software acquisition, and help desks). This also relates to OMB's PortfolioStat initiative and a CIO-lead business approach to the delivery of IT infrastructure, enterprise IT, and administrative/business systems that emphasizes pooling Agencies' purchasing power across their entire organization through shared

Term	Source Document	Definition
		services as a provider or consumer, instead of standing up separate independent services to eliminate duplication, rationalize the Agency's IT Investments, and drive down costs. There are three categories of Commodity IT: • Enterprise IT – Items that pertain to this are: E-mail; Collaboration; Identity and Access Management; IT Security (Not Identity and Access Mgmt.); and Web Hosting, Infrastructure, and Content. • IT Infrastructure - Items that pertain to this are: Desktop Systems; Mobile Devices; Mainframes and Servers; and Telecommunications. • Business Systems - Items that pertain to this are: Financial Management; Human Resources Management; Grants-Related Federal Financial Assistance; Grants-Related Transfer to State and Local Governments (see http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/shared_services_strategy.pdf).
Community Cloud	NIST Special Publication 800-145 -The NIST Definition of Cloud Computing	This term refers to cloud computing technology in which the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises (see NIST Special Publication 800-145 -The NIST Definition of Cloud Computing http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf).
Contributions (or Expected Contributions)	IT Budget - Capital Planning Guidance	This term refers to both monetary contributions, or a dollar-equivalent of In-kind services and fees for services provided by a partner Agencies/sub-Agencies to managing partners or shared service providers. Contributions can collected from partner Agencies or partner sub-Agencies by either Multi-Agency collaborations or Intra-Agency shared services. • Contributions represents the sum portion for all funds collected by the managing partner of the shared service. • Fee-for-service (a type of contribution) are typically use the Economy Act, 31 U.S.C. § 1535 as the authorization for the transfer of funds. Other monetary contributions or in-kind equivalents contributions typically use the Clinger-Cohen Act of 1996, 40 U.S.C. § 1424.
Cost	Capital Planning Guide	Defined in Statement of Federal Financial Accounting Concepts (SFFAC) No. 1, Objectives of Federal Financial Reporting, as the monetary value of resources used. Defined more specifically in Statement of Federal Financial Accounting Standards (SFFAS) No. 4, Managerial Cost Accounting Concepts and Standards for

Term	Source Document	Definition
		the Federal Government, as the monetary value of resources used or sacrificed or liabilities incurred to achieve an objective, such as to acquire or produce a good or to perform an activity or service. Depending on the nature of the transaction, cost may be charged to operations immediately (i.e., recognized as an expense of the period) or to an asset account for recognition as an expense of subsequent periods. In most contexts within SFFAS No. 7, Accounting for Revenue and Other Financing Sources, "cost" is used synonymously with expense.
Cost Avoidance	OMB Circular A-131	An action taken in the immediate time frame that will decrease costs in the future. For example, an engineering improvement that increases the mean time between failures and thereby decreases operation and maintenance costs is a cost avoidance action (as defined in OMB Circular A-131 http://www.whitehouse.gov/omb/circulars_a131).
Cost Savings	OMB Circular A-131	Cost Saving refers to the reduction in actual expenditures to achieve a specific objective (as defined in OMB Circular A-131 http://www.whitehouse.gov/omb/circulars_a131).
Critical Path	OMB E-Gov	An activity in which a delay in completion causes a corresponding delay in the ultimate completion of the project by at least an equal amount of time.
Data Center	Forthcoming OMB CIO Memo, "Data Center Optimization Initiative"	"For the purposes of this memorandum, rooms with at least one server, providing services (whether in a production, test, staging, development, or any other environment), are considered data centers. However, rooms containing only print servers, routing equipment, switches, security devices (such as firewalls), or other telecommunications components shall not be considered data centers."
Dataset	OMB Memo M-13-13	This term refers to a collection of structured data presented in tabular or non-tabular form (per OMB M-13-13 Open Data Policy-Managing Information as an Asset) (http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf).
Defense Acquisition Workforce Improvement Act (DAWIA) of 1990 (P.L. 101-510)	IT Budget - Capital Planning Guidance	DAWIA of 1990 (P.L. 101-510) refers to a congressional act that established for the Department of Defense an Acquisition Corps to professionalize the acquisition workforce in the DoD through education, training, and work experience.
Dependency	IT Budget - Capital Planning Guidance	Dependency refers to the identification of relationships between projects and operational assets within an Investment as well as the identification of relationships between Investments. Action taken by one affects the other. Identification of dependencies is critical to the management of project, program, and portfolio risk.
Desktop and Laptop systems	OMB Circular A-11 (2010)	Desktop and Laptop systems are defined as "End User Systems" that can consist of any of the following: desktops and laptops, printers (both individual and

Term	Source Document	Definition
		shared), print servers; and scanners. This category includes the local hardware and software (PC operating systems, office automation suites) cost associated with the device as well as any related support costs (excluding help desk). • Desktops and laptops • Peripherals (scanners, fingerprint scanners, etc.) • Software/Desktop Applications (PC operating systems, office automation suites) • Local printers, shared printers, fax machines or the cost of supplies (e.g., toner and paper)
Development, Modernization, and Enhancement (DME)	IT Budget - Capital Planning Guidance	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.
Disposition Cost	IT Budget - Capital Planning Guidance	Disposition Cost refers to the cost of retiring a capital asset once its useful life is completed or a replacement asset has superseded it; disposition costs may be included in operational activities near the end of the useful life of an asset.
Earned Value Management (EVM)	American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) Standard–748–1998, Earned Value Management Systems. Additional information on EVMS is available at www.acq.osd.mil/evm.	EVM refers to an integrated management system that coordinates the work scope, schedule, and cost goals of a program or contract, and objectively measures progress toward these goals. EVM is a tool used by program managers to: (1) quantify and measure program/contract performance, (2) provide an early warning system for deviation from a baseline, (3) mitigate risks associated with cost and schedule overruns, and (4) provide a means to forecast final cost and schedule outcomes. The qualities and operating characteristics of earned value management systems (EVMS) are described in American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) Standard–748–1998, Earned Value Management Systems. Additional information on EVMS is available at www.acq.osd.mil/evm.
E-mail	FEA Consolidated Reference Model Document, Version 2.3	Electronic mail is the exchange of computer generated and stored messages by telecommunication. An e-mail can be created manually via messaging applications or dynamically/ programmatically such as automated response systems. For Agencies that have outsourced e-mail services to another Agency or vendor, this is the obligation for e-mail related costs.

Term	Source Document	Definition
		• Costs should include the full cost of the e-mail solution including software licenses, server and communications hardware, equipment, data center allocation/charges, storage, backup solution, and contractors. • Does not include the cost of the end user client computing device/software or the telecommunications cost for the LAN/WAN/wireless costs.
End of Life	IT Budget - Capital Planning Guidance	The original equipment manufacturer or software vendor is no longer providing spare parts or support for the particular software version.
Enterprise Architecture (EA)	OMB Circular A-130	This term refers to the strategic, business, and technology and documentation of the current and desired relationships among business and management processes and IT of an organization. An EA includes the rules and standards and systems life cycle information to optimize and maintain the environment which the Agency wishes to create and maintain through its IT portfolio. An EA must provide a strategy that enables the Agency to support its current state and provides a roadmap for transition to its target environment. An EA defines principles and goals and sets a direction on such issues as the promotion of interoperability, open systems, publics access, end-user satisfaction, and IT security.
Enterprise Roadmap	OMB Memo M-13-09	This term refers to a document that describes the business and technology plan for the entire organization using EA methods. The Roadmap provides current views, future views, and transition plans at an appropriate level of detail for all IT Investments, services, systems, and programs. The Enterprise Roadmap also contains an IT asset inventory using the FEA Reference Models and other attachments or appendices for CPIC, EA, shared service, and other planning products requested by OMB that provide additional information regarding Roadmap plans. http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-09.pdf - page 4.
Epic	Forthcoming Agile Development Guidance	An Epic is the total number of sprints needed to complete a release as determined by Product Owner or Manager. Example: Release 1: Epic 1: Sprint 1 User Stories 1-4 Sprint 2 User Stories 5-8
Evaluation (by Agency CIO)	IT Budget - Capital Planning Guidance	This term refers to the CIO's best judgment of the current level of risk for an Investment in terms of its ability to accomplish its goals (40 U.S.C. § 11315(c)(2)). The evaluation should be informed by the following factors, including, but not limited to: risk management, requirements management, contractor oversight, historical performance, human capital and other factors that the CIO deems important to the forecasting future success. Each evaluation should include narrative to

Term	Source Document	Definition
		address/explain the rating. This is particularly important whenever the rating has changed since the last evaluation.
Federal Acquisition Certification for Program and Project Managers (FAC-P/PM)	FAC-P/PM	Federal Acquisition Certification for Program and Project Managers (FAC-P/PM) refers to a certification program that was established to clearly identify general training and experience requirements for program and project managers (PMs) in civilian Agencies. The FAC-P/PM focuses on essential competencies needed for program managers and PMs. The certification program does not include functional or technical competencies, such as those for IT or Agency-specific competencies. Defense Agencies have a similar certification program under DAWIA. Agencies were required to be compliant with FAC-P/PM starting in FY 2008. Available levels are Entry/Apprentice, Mid/Journeyman, and Expert/Advanced for FAC-P/PM and 1, 2, and 3 for DAWIA. For more information about these programs, refer to the following links: http://www.whitehouse.gov/sites/default/files/omb/procurement/workforce/fed_acq_cert_042507.pdf, http://whitehouse.gov/omb/procurement/acq_wk/fac_contracting_program.pdf, http://www.whitehouse.gov/sites/default/files/omb/procurement/memo/fac-ppm-revised-dec-2013.pdf.
Federal Enterprise Architecture (FEA)	IT Budget - Capital Planning Guidance	This term refers to a business-based documentation and analysis framework for Agency and government-wide improvement. The FEA provides standardized methods to describe the relationship between an Agency's strategic goals, business functions, and enabling technologies at various levels of scope and complexity. The FEA is comprised of documentation in six domain areas (strategic goals, business services, data and information, systems and applications, infrastructure, and security) that includes required and elective artifacts. More information about the FEA is available in The Common Approach to Federal Enterprise Architecture (OMB, May 2, 2012) and at FEA Reference Model document library.
FEA Mapping Codes	FEA Consolidated Reference Model Document, Version 2.3	This term refers to the unique identifiers for the information contained in the FEA Reference Models. The mapping codes are used to align information reported by Agencies back to a common FEA taxonomy. Use of the Reference Models provides a common vocabulary and framework to relate information captured across the Federal Government. The first three-digit code indicates the primary service area served by this Investment (the three-digit BRM service code). The second through fifth three-digit codes indicate the secondary services associated with this Investment. Guidance on the codes for these mappings can be found at FEA Reference Model document library.

Term	Source Document	Definition
Federal IT Dashboard (ITDB)	www.itdashboard.gov	This term refers to a website (www.itdashboard.gov) that enables Federal Agencies, industry, the general public, and other stakeholders to view details regarding the performance of Federal IT Investments. The ITDB is used by the Administration and Congress to inform budget and policy decisions.
Financial Management Systems	OMB Circular A-127	This term refers to systems necessary to support financial management, including automated and manual processes, procedures, controls, data, hardware, software, and support personnel dedicated to the operation and maintenance of system functions. The following are examples of financial management systems: core financial systems, procurement systems, loan systems, grants systems, payroll systems, budget formulation systems, billing systems, and travel systems (see OMB Circular A-127 for additional information and guidance at www.whitehouse.gov/omb/circulars_a127).
Full Funding	OMB Circular A-11	Full Funding means appropriations are enacted sufficient to complete a useful segment of a capital project or Investment (or the entire project or Investment, if it is not divisible into useful segments) before any obligations for the useful segment (or project or Investment) may be incurred. Incrementally funding the planning and acquisition of capital assets (or useful segments), without certainty if or when future funding will be available, can result in poor planning, inadequate justification of asset acquisition, higher acquisition costs, cancellation of projects, the loss of sunk costs, or inadequate funding to maintain and operate the assets. Requests for procurement programs must provide for full funding of the entire cost (see Section 31.5 of OMB Circular A-11 and the Capital Programming Guide).
Functional/Business Sponsor	IT Budget - Capital Planning Guidance	This term refers to the Agency official who is responsible for the program or function supported or implemented by the Investment (44 U.S.C. § 3501 (a)(4)). The sponsor is responsible for expressing the value of, ensuring successful implementation of, and providing accurate and timely data for the IT Investment to the Agency CIO and OMB. The designated person may (or may not) be the same as the "Business Process owner/Subject Matter Expert" serving on the IPT. Each major and non-major IT Investment must include the name of the functional/business sponsor as well as the individual's title.
Funding	Capital Planning Guide	There are two types of funding for projects: (1) Full funding means that appropriations are enacted that are sufficient in total to complete a useful segment of a capital project (Investment) before any obligations may be incurred for that segment. When capital projects (Investments) or useful segments are incrementally funded, without certainty if or when future funding will be available, it can result in poor planning, acquisition of assets not fully justified, higher acquisition costs, projects (Investments) delays, cancellation of major

Term	Source Document	Definition
		projects (Investments), the loss of sunk costs, or inadequate funding to maintain and operate the assets. Budget requests for full acquisition propose for full funding. (2) Incremental (annual) funding means that appropriations are enacted that only fund an annual or other part of a useful segment of a capital project (Investment). OMB or the Congress may change the Agency's request for full finding to incremental funding in order to accommodate more projects in a year than would be allowed with full funding.
Funding Source	IT Budget - Capital Planning Guidance	Funding Source refers to the direct appropriation or other budgetary resources an Agency receives for an IT Investment. When "original paying accounts" within Agencies are transferring resources to a different Agency account that ultimately supports the IT Investment (for example, when bureau accounts are paying into a central CIO office account or a working capital fund), the funding source provided in Agency IT Investment Portfolio should be the account that ultimately pays contracts and other costs for the Investment directly (not the original account(s) for the funds); the point of execution. Note: For Agencies on the ITDB, funding sources are planned as the primary drivers in the algorithm to display "spending by bureau," rather than using the bureau code associated with Investments. It is critical that valid OMB Budget Account (funding source) codes be provided for each funding source in Agency submissions.
Funding Transfer Investment	IT Budget - Capital Planning Guidance	This term refers to the portion of funding a partner Agency provides funding contributions to another IT Investment. The description of the IT Investment should indicate the UII of the managing partner Investment.
Government Information	OMB Circular A-130	Government Information refers to information created, collected, processed, disseminated, or disposed of by or for the Federal Government (see http://www.whitehouse.gov/omb/circulars_a130)
Gross Savings	IDC	The amount of cost savings (per Circular A-131) on an annual basis without taking into account the one-time costs of implementing the cost savings or cost avoidance strategy (as defined in OMB Circular A-131 http://www.whitehouse.gov/omb/circulars_a131).
Help desk (End User Support)	FEA Business Reference Model v 3.0	Help Desk Services involves the operation of a service center to respond to government and contract employees' end user device and software support needs (includes, but is not limited to, costs related to employees, contractors, and ticket management software).
Hybrid Cloud	NIST Special Publication 800-145 -The NIST Definition of Cloud Computing	Cloud computing technology in which the cloud infrastructure is a combination of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds) (see NIST Special Publication

Term	Source Document	Definition
		800-145 -The NIST Definition of Cloud Computing http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf for official government definition).
Identity and Access Management	OMB Circular A-11 (2010)	Includes funding of activities required to implement HSPD-12 and the Federal Identity, Credentialing and Access Management (FICAM) roadmap segment architecture requirements as directed by OMB. This includes but is not limited to HSPD-12 PIV Card deployment and operations, logical PIV Card access implementations, to include network and application access, identity management systems, physical access control systems, etc. • Costs include all IT related to identity and access management including cost of PIV cards, certificates, software licenses, server and communications hardware, equipment, data center allocation/charges, storage, backup solution and contractors.
Information Resources Management (IRM) Strategic Plan	44 U.S.C. § 3506(b)(2); OMB Circular A-130	IRM Strategic Plan refers to a document that addresses all information resources management of an Agency. Agencies must develop and maintain their IRM strategic plans as required by 44 U.S.C. § 3506(b)(2) and OMB Circular A-130. IRM strategic plans should support the Agency's strategic plan that is required in OMB Circular A-11; provide a description of how information resources management activities help accomplish the Agency's missions delivery area and program decisions; and ensure IRM decisions are integrated with management support areas, including organizational planning, budget, procurement, financial management, and human resources management.
Information Security	OMB Memo M-04-25	This term refers to all functions pertaining to the protection of federal information and information systems from unauthorized access, use, disclosure, disruptions, modification, or destruction, as well as the creation and implementation of security policies, procedures and controls. It includes the development, implementation, and maintenance of security policies, procedures, and controls across the entire information life cycle. These functions should include implementation and activities associated with NIST 800-37, Security Awareness training (but not the technical infrastructure required for the delivery of training), FISMA compliance reporting, development of a security policy, and security audits and testing. • IT security should include systems that oversee Agency IT needs. • Do Not Include IT costs related to Identity or Access Management systems/solutions. • Do Not Include physical protection of an organization (e.g., guards, cameras, and facility protection). http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-25.pdf and FISMA, section 3542(b)(1)(A-C)

Term	Source Document	Definition
Information System	44 U.S.C. § 3502; OMB Circular A-130	Information System refers a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, transmission, or dissemination of information, in accordance with defined procedures, whether automated or manual (see http://www.whitehouse.gov/omb/circulars_a130_a130trans4, http://www.gpo.gov/fdsys/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap35-subchapI-sec3502.pdf).
Information Technology (IT)	OMB Memo M-15-14 https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf	IT is defined as: A. Any 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; where B. such services or equipment 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 either use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product. C. IT 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 life cycle of the equipment or service), and related resources. D. IT does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment.
IT Investment	OMB Circular A-11 Section 55	This term refers to the expenditure of IT resources to address mission delivery and management support. An IT Investment may include a project or projects for the development, modernization, enhancement, or maintenance of a single IT asset or group of IT assets with related functionality, and the subsequent operation of those assets in a production environment. All IT Investments should have a defined life cycle with start and end dates, with the end date representing the end of the currently estimated useful life of the Investment, consistent with the Investment's most current alternatives analysis if applicable. When the asset(s) is essentially replaced by a new system or technology, the replacement should be reported as a new, distinct Investment, with its own defined life cycle information.

Term	Source Document	Definition
IT Program Managers and IT Project Managers	IT Budget - Capital Planning Guidance	IT Program Managers and IT Project Managers refers to the IPT members responsible for IT Investments and lead the required IPT for the Investment. In some cases, IT program managers and PMs can hold positions in other classification series; however they must still meet the requisite Federal certification and/or IT program management experience requirements. Further definitions are available in the Office of Personnel Management's Job Family Standard for Administrative Work in the Information Technology Group (series 2200 in the Federal Classification and Job Grading Systems).
IT Resources	OMB Memo M-15-14 https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf	IT Resources is defined as: A. All 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 life cycle of IT; B. acquisitions or Inter-Agency agreements that include IT and the services or equipment provided by such acquisitions or Inter-Agency agreements; but C. does not include grants to third parties which establish or support IT not operated directly by the Federal Government.
IT Systems for National Security	40 U.S.C. § 5141 & 5142	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which: 1. involves intelligence activities; 2. involves cryptologic activities related to national security; 3. involves command and control of military forces; 4. involves equipment that is an integral part of a weapon or weapons system; or 5. subject to subsection (b), is critical to the direct fulfillment of military or intelligence missions. (b) LIMITATION. Subsection (a)(5) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). National Security Systems are required to report as a part of the Capital Planning process.
Infrastructure as a Service (IaaS) Cloud Computing	NIST Special Publication 800-145 -The NIST Definition of Cloud Computing	The capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls) (see NIST Special Publication 800-145 -The NIST Definition of Cloud Computing

Term	Source Document	Definition
		http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf for official government definition).
Integrated Program/ Project Team (IPT)	Capital Planning Guide	A multi-disciplinary team led by a program/project manager responsible and accountable for planning, budgeting, procurement and life-cycle management of the Investment to achieve its cost, schedule, and performance goals. Team skills include: budgetary, financial, capital planning, procurement, user, program, architecture, earned value management, security, and other staff as appropriate. In order for OMB to approve the Investment budget, an IPT must include at a minimum: a qualified, fully dedicated IT program manager; a contracting specialist, if applicable; an IT specialist; an IT security specialist; and a business process owner or subject matter expert (SME). Other members of the IPT might include enterprise architects; IT specialists with specific expertise in data, systems, or networks; capital planners; or performance specialists. Key members of the IPT should be co-located during the most critical junctures of the program, to the maximum extent possible. Agencies should establish IPT members' individual performance goals to hold team members accountable for both individual functional goals and the overall success of the program. The Investment IPT should be defined in a program or an IPT charter.
Inter-Agency Acquisition	31 U.S.C. § 1535	Inter-Agency Acquisition refers to the use of the Federal Supply Schedules; a Multi-Agency contract (i.e., a task order or delivery order contract established by one Agency for use by multiple government Agencies to obtain supplies and services, consistent with the Economy Act, 31 U.S.C. § 1535) or a government-wide acquisition contract (i.e., a task order or delivery order contract for IT established by one Agency for Government-wide use operated by an executive agent, as designated by OMB pursuant to Section 11302(3) of the Clinger-Cohen Act of 1996).
IT Asset	Capital Programming Guide	This term refers to anything (tangible or intangible) that has value to an organization, including, but not limited to: a computing device, IT system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards) as well as people and intellectual property (including software). Assets are the lowest level at which IT is planned, acquired, implemented, and operated.
IT Management Investment	IT Budget – Capital Planning Guidance	A standard Investment category to capture all costs associated with IT Management and Strategic Planning (including CIO and other senior leadership FTE costs), Enterprise Architecture, Capital Planning, Project Management Offices, IT Budget/Finance, and IT Vendor Management, 508 Compliance, general IT policy and reporting, and IT Governance. This may include Investments mapped to FEA BRM "Executive Direction and Management."

Term	Source Document	Definition
IT Migration Investment	IT Budget - Capital Planning Guidance	This term refers to the migration costs associated with systems in a Shared Service partner Agency that are not captured by the managing partner when the partner Agency is migrating to the shared system. The description of the IT Investment should indicate the UII of the major IT Investment of the managing partner.
IT Security and Compliance Investment	IT Budget - Capital Planning Guidance	A standard Investment category to capture all costs associated with IT Security resources setting policy, establishing process and means, and measuring compliance and responding to security breaches. Additionally, the Investment captures costs associated with IT compliance such as establishing controls and measuring compliance to relevant legal and compliance requirements. The Investment also includes costs associated with privacy but does not include mission (non-IT) security and compliance.
IT Service	ISO 20000	A means of delivering IT, in combination with any inherent people or processes, of value to customers by facilitated outcomes customers want to achieve without the ownership of specific costs and risks. (See: ISO 20000 - https://www.iso.org/obp/ui/#iso:std:iso-iec:20000:-1:ed-2:v1:en)
Iteration / Sprint	Agile Development Guidance	A distinct sequence of activities with a baselined plan and valuation criteria resulting in a release.
Life Cycle Costs	Capital Programming Guide; OMB Circular A-131	Life Cycle Costs refers to all Investment costs (including government FTEs) from the commencement of the Investment through its estimated useful life (or the composite estimated useful life of the assets within the Investment), independent of the funding source (e.g., revolving fund, appropriated fund, working capital fund, trust fund). For more information about life cycle costs, see the Capital Programming Guide of OMB Circular A-11 and OMB Circular A-131.
Mainframes and Servers	OMB Circular A-11 (2010)	This term refers to a subset of the Mainframes and Servers Systems & Support apportionment category. The definition for this data center commodity IT area applies equally to any data processing environment (such as production, backup, DR/COOP, test, development, etc.) and typically includes: • Hardware (storage controllers, storage servers): Includes all dedicated storage hardware devices such as controllers, servers, disk arrays, tape libraries, and optical jukeboxes, as well as supplies (media) used to store data offline such as tapes. • Software: Includes software dedicated to managing the storage systems, including creation and setup, storage maintenance, reporting, security, monitoring, backup/restore, archival, replication, media handling and data migration/tiering. • Disaster recovery: Includes the hardware, software, facilities and contracts specifically dedicated to disaster recovery for storage management. • Outsourcing: Includes third party and outsource

Term	Source Document	Definition
		contracts, such as managed storage services and cloud-based storage. • Personnel: In-house costs for government personnel (salaries and benefits) and costs for contract personnel supporting operations/maintenance, engineering/technical services, planning and process management, services administration, management and administration allocated to storage systems.
Maintenance	Federal Accounting Standards Advisory Board Statement of Federal Financial Accounting Standards Number 10	Maintenance refers to the activity necessary to keep an asset functioning as designed during the O&M phase of an Investment. Maintenance activities may also include, but are not limited to, operating system upgrades, technology refreshes, and security patch implementations. Some maintenance activities should be managed as projects and reported in Section B of Major IT Investment Update. As defined in the Federal Accounting Standards Advisory Board Statement of Federal Financial Accounting Standards Number 10, maintenance excludes activities aimed at expanding the capacity of an asset or otherwise upgrading it to serve needs different from or significantly greater than those originally intended.
Major IT Investment	OMB Memo M-15-14 https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf	An IT Investment requiring special management attention because of its importance to the mission or function to the government; significant program or policy implications; high executive visibility; high development, operating, or maintenance costs; unusual funding mechanism; or definition as major by the Agency's CPIC process. Agencies should also include all "major automated information system" as defined in 10 U.S.C. § 2445 and all "major acquisitions" as defined in the OMB Circular A-11 Capital Programming Guide consisting of information resources. OMB may work with the Agency to declare IT Investments as major IT Investments. Agencies must consult with assigned OMB desk officers and Resource Management Offices (RMOs) regarding which Investments are considered "major." Investments not considered "major" are "non-major."
Managing Partner	Federal IT Shared Services Strategy, May 2, 2012	This term refers to the lead Agency that is responsible for coordinating the implementation of the E-Gov or LoB initiative. The managing partner maintains an IT shared service with approval by Agency leadership for Intra-Agency services, and also by OMB for Inter-Agency services. The Managing Partner organization, often referred to as the Program Management Office (PMO), develops, implements, and maintains financial and service models as well as contracts with Customers and Suppliers using strategic sourcing vehicles whenever practicable. The Managing Partner PMO is responsible for the success of the IT shared service, and reports using metrics developed by the Federal Agency for its own Intra-Agency IT shared services, and by the Federal CIO Council's Shared Services Subcommittee for Inter-

Term	Source Document	Definition
		Agency LoB. Managing Partners are also responsible for maintaining contracts with Customer Agencies that allow the Customer Agency to terminate the contract if specified levels of service are not maintained (http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/shared_services_strategy.pdf).
Modular Development	Contracting Guidance to Support Modular Development, June 14, 2012	An approach that focuses on the delivery of specific Investments, projects, or activities of an overall capability by progressively expanding upon delivered capabilities until the full capability is realized. Investments may be decomposed into discrete projects, increments, or useful segments, each of which is undertaken to develop and implement products and capabilities that the larger Investment delivers. For more information, see Contracting Guidance to Support Modular Development (OMB, June 14, 2012).
Mobile Devices	OMB Circular A-11 (2010)	Total non-desktop, non-laptop, small form factor wireless end user device costs, including: hardware (including handsets, tablets, and wireless modems such as air cards), software, labor, maintenance, and service (including network service, such as cellular voice and data plans). Help desk costs should not be included here.
Net Savings	OMB Circular A-131	The amount of cost savings (per Circular A-131) minus the cost required to implement and operate the cost savings or cost avoidance strategy.
Network storage	OMB Circular A-130	Applies to any data processing environment (such as production, backup, DR/COOP, test, development, etc.) and includes: • Hardware (storage controllers, storage servers): Includes all dedicated storage hardware devices such as controllers, servers, disk arrays, tape libraries, and optical jukeboxes, as well as supplies (media) used to store data offline such as tapes. • Software: Includes software dedicated to managing the storage systems, including creation and setup, storage maintenance, reporting, security, monitoring, backup/restore, archival, replication, media handling and data migration/tiering. • Disaster recovery: Includes the hardware, software, facilities and contracts specifically dedicated to disaster recovery for storage management. • Outsourcing: Includes third party and outsource contracts, such as managed storage services and cloud-based storage. • Personnel: In-house costs for government personnel (salaries and benefits) and costs for contract personnel supporting operations/maintenance, engineering/technical services, planning and process management, services administration, management and administration allocated to storage systems. *Note*: Dollars should only appear in ONE category, for example network storage OR mainframes and servers.

Term	Source Document	Definition
New IT Investment	IT Budget - Capital Planning Guidance	This term refers to an IT Investment and its associated projects that is newly proposed by the Agency and that has not been previously reported/funded by OMB. An asset(s) within an Investment that is essentially replaced by a new system or technology may be reported as a new, distinct Investment, with its own defined life cycle costs, or may be included within the current Investment.
Non-Major IT Investment	IT Budget - Capital Planning Guidance	This term refers to any IT Investment in the Agency's IT Portfolio that does not meet the definition of "major IT Investment" (01), "Funding Transfer Investment" (04) or "IT Migration Investment" (03). All non-major IT Investments must be reported in the Agency IT Investment Portfolio. For more details see section 10 of CPIC IT Portfolio Guidance.
Ongoing IT Investment	IT Budget - Capital Planning Guidance	Ongoing IT Investment refers to an Investment and its associated assets, including both maintenance projects and operational activities, that has been through a complete Budget Cycle with OMB with respect to the President's Budget for the current year (CY) — in this case, for FY 2017.
Operational Analysis	Capital Planning Guide; GAO-13-87	This term refers to a method of examining the ongoing performance of an operating asset Investment and measuring that performance against an established set of cost, schedule, and performance goals. An operational analysis is, by nature, less structured than performance reporting methods applied to developmental projects and should trigger considerations of how the Investment's objectives could be better met, how costs could be reduced, and whether the organization should continue performing a particular function. Guidance for Operational Analysis is described in the Capital Programming Guide. Best Practices can also be found in GAO's GAO-13-87 report (http://www.gao.gov/assets/650/649563.pdf).
Operations	OMB Circular A-130, IT Budget - Capital Planning Guidance	This term refers to the day-to-day management of an asset in which the asset is in operations production environment and produces the same product or provides a repetitive service. Operations include, but are not limited to, activities that operate data centers, help desks, operational centers, telecommunication centers, and end-user support services. Operational activities are located in Section C of the Major IT Investment Update part of the FY16 CPIC Guidance.
Operations and Maintenance (Steady State) Costs	IT Budget - Capital Planning Guidance	Operations & Maintenance Costs refers to the expenses required to operate and maintain an IT asset that is operating in a production environment. O&M costs include costs associated with operations, maintenance activities, and maintenance projects needed to sustain the IT asset at the current capability and performance levels. It includes Federal and contracted labor costs, corrective hardware and software maintenance, voice and data communications maintenance and service, replacement of broken or obsolete IT equipment, overhead costs, business operations and commercial services costs, and

Term	Source Document	Definition
		costs for the disposal of an asset. Also commonly referred to as steady state.
Partner (Customer) Agency	Federal IT Shared Services Strategy, May 2, 2012	This term refers to the Agency in an inter/intra Agency collaboration (such as an E-Gov or LoB initiatives or a shared services). The Federal Agency or sub-organization that contracts with and pays a Managing Partner to receive an IT shared service. The Customer Agency organization may be required to interact with a Supplier for the coordination of day-to-day service issues. The Managing Partner handles major contract issues and resolves escalation items with Suppliers. The Partner Agency usually provides resources (e.g., funding, FTEs, in-kind) for the management, development, deployment, or maintenance of a common solution. The partner Agency is also responsible for including the appropriate line items in its own Agency IT Investment Portfolio budget submission, and reflecting the amount of the contribution for each of the initiatives to which the Agency provides resources. http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/shared_services_strategy.pdf.
Performance Reference Model (PRM)	FEA Consolidated Reference Model Document Version 2.3; GPRA 2010 Public Law 111-352	PRM refers to one of six reference models of the FEA. The PRM allows Agencies to better manage the business of government at a strategic level, by providing a means for using the EA to measure the success of Investments and their impact on strategic outcomes. The PRM establishes a line of sight to outcomes and a common language to describe the outputs and measures used to achieve strategic objectives through coupled business services (mission and support). The PRM shows the linkage between internal business components and the achievement of business and customer-centric outputs and outcomes. Most importantly, the PRM helps to support planning and decision-making based on comparative determinations of which programs and services are more efficient and effective. The PRM is both a taxonomy and a standard method for performance measurement as it provides for a common approach to performance and outcome measurements throughout the Executive Branch of the Federal Government, as is required by the Government Performance and Results Modernization Act of 2010 (P.L. 111-352). Current PRM service codes can be found in PRM version 3.
Performance-Based Acquisition Management	FAR 37.101	Performance-Based Acquisition Management refers to a documented, systematic process for program management, which includes the integration of program scope, schedule and cost objectives, the establishment of a baseline plan for accomplishment of program objectives, and the use of earned value techniques for performance measurement during execution/acquisition of the program. This type of management includes prototypes and tests to select the most cost-effective alternative during the planning phase; the work during the acquisition phase; and any developmental, modification, or upgrade work done during the O&M

Term	Source Document	Definition
		phase. A performance-based acquisition (as defined in the FAR 37.101) or contract/agreement with a defined quality assurance plan that includes performance standards/measures should be the basis for monitoring contractor or in-house performance of this phase.
Planning	40 U.S.C. § 11315; OMB Circular A-130	Planning refers to preparing, developing, or acquiring the information used to design the asset; assess the benefits, risks, and risk-adjusted costs of alternative solutions; and establish realistic cost, schedule, and performance goals for the selected alternative, before either proceeding to full acquisition of the capital project or useful component or terminating the project. Planning must progress to the point where the Agency is ready to commit to achieving specific goals for the completion of the acquisition before proceeding to the acquisition phase. Information gathering activities to support planning may include market research of available solutions, architectural drawings, geological studies, engineering and design studies, and prototypes. Planning may be general to the overall Investment or may be specific to a useful component. For Investments developed or managed using an incremental or agile methodology, planning will be conducted throughout the entire acquisition, focusing on each iteration/sprint.
Platform as a Service (PaaS) Cloud Computing	NIST Special Publication 800-145 -The NIST Definition of Cloud Computing	The capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment (NIST Special Publication 800-145 -The NIST Definition of Cloud Computing http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf).
PortfolioStat Review	OMB memo M-13-09; FY13 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management	PortfolioStat refers to a face-to-face, evidence-based review of an Agency's IT portfolio. Reviews can be used to identify and address a broad range of issues, including management of commodity IT, duplication of Investments, and alignment with the Agency's mission and strategy. More detail regarding the PortfolioStat process is described in OMB memo M-13-09 – Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management
Post-Implementation Review (PIR)	Capital Programming Guide; OMB Circular A-130	PIR refers to an evaluation of how successfully the Investment or project objectives were met and how effective the project management practices were in keeping the Investment or project on track. A PIR can be conducted after a project has been completed, or after an Investment concludes the implementation phase. Additional details regarding the PIR process is described in the Capital Programming Guide.

Term	Source Document	Definition
Privacy Impact Assessment	OMB Memo M-03-22	Privacy Impact Assessment is a process for examining the risks and ramifications of using IT to collect, maintain, and disseminate information from or about members of the public in an identifiable form. The process also is also used to identify and evaluate protections and alternative processes to mitigate the impact to privacy of collecting such information. Consistent with OMB guidance M-03-22 regarding implementing the privacy provisions of the E-Government Act, Agencies must conduct and make publicly available PIAs for all new or significantly altered IT Investments that administer information in an identifiable form collected from or about members of the public.
Private Cloud	NIST Special Publication 800-145 -The NIST Definition of Cloud Computing	Cloud computing technology in which the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. (NIST Special Publication 800-145 -The NIST Definition of Cloud Computing http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf)
Product Backlog	Forthcoming Agile Development Guidance	This term refers to a comprehensive to-do list, expressed in priority order based on the business value each piece of work will generate.
Product Owner	Forthcoming Agile Development Guidance	The Product Owner is responsible for maximizing the value of the product and the work of the Development Team. The Product Owner is the sole person responsible for managing the Product Backlog. Product Backlog management includes: Clearly expressing Product Backlog items; Ordering the items in the Product Backlog to best achieve goals and missions; Optimizing the value of the work the Development Team performs; Ensuring that the Product Backlog is visible, transparent, and clear to all, and shows what the Scrum Team will work on next; and, Ensuring the Development Team understands items in the Product Backlog to the level needed. The Product Owner may do the above work, or have the Development Team do it. However, the Product Owner remains accountable. The Product Owner is one person, not a committee. The Product Owner may represent the desires of a committee in the Product Backlog, but those wanting to change a Product Backlog item's priority must address the Product Owner. For the Product Owner to succeed, the entire organization must respect his or her decisions. The Product Owner's decisions are visible in the content and ordering of the Product Backlog. No one is allowed to

Term	Source Document	Definition
		tell the Development Team to work from a different set of requirements, and the Development Team isn't allowed to act on what anyone else says.
Project	40 U.S.C. § 11315; OMB Circular A-130	This term refers to a temporary endeavor undertaken to accomplish a unique product or service with a defined start and end point and specific objectives that, when attained, signify completion. Projects can be undertaken for the development, modernization, enhancement, disposal, or maintenance of an IT asset. Projects are composed of activities. When reporting project status, to the maximum extent practicable, Agencies should detail the characteristics of "increments" under modular contracting as described in the Information Technology Management Reform Act of 1996 (ITMRA, also known as the "Clinger-Cohen Act") and the characteristics of "useful segments," as described in OMB Circular A-130.
Project Manager Level of Experience	Federal IT Project Manager Guidance Matrix published by the CIO Council (https://cio.gov/wp-content/uploads/downloads/2013/08/Federal-IT-PM-Guidance-Matrix2.ppt).	This term refers to the specific certification(s) or number of years of direct project management experience that the PM holds. Examples of PM certifications include FAC-P/PM, Project Management Institute's Project Management Professional (PMP), and other recognized certifications. Refer to Federal IT Project Manager Guidance Matrix published by the CIO Council (https://cio.gov/wp-content/uploads/downloads/2013/08/Federal-IT-PM-Guidance-Matrix2.ppt).
Provisioned IT Service	IT Budget - Capital Planning Guidance	Provisioned IT Service is a new category of funds that must be reported as appropriate. A "Provisioned IT Service" refers to an IT service that is (1) owned, operated, and provided by an outside vendor or external government organization (i.e., not managed, owned, operated, and provided by the procuring organization) and (2) consumed by the Agency on an as-needed basis. Provisioned IT services are considered subcategories of DME and O&M. Examples of Provisioned IT Service may include the purchase of E-Gov LoB from another Federal Agency, or the purchase of SaaS, PaaS, IaaS from a private service provider, or the purchase of shared services or cloud services. Provisioned IT Service excludes Software Licenses but includes both Intra-Agency and Inter-Agency Shared Services.
Public Cloud	NIST Special Publication 800-145 -The NIST Definition of Cloud Computing	Cloud computing technology in which the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. (NIST Special Publication 800-145 -The NIST Definition of Cloud Computing http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf)
Records	44 U.S.C. § 3502; OMB Circular A-130	Records refers to all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an Agency of the United States Government under Federal law or in connection with the

Term	Source Document	Definition
		transaction of public business. Records may also include items that are preserved or appropriate for preservation by that Agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Federal Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and processed documents are may not be included as records.
Release	Forthcoming Agile Development Guidance	A Release is a release of a product that is shipped to the customer. Each development project has a set number of releases, and within the releases can be multiple versions if that is how the Product Owner or Manager sets up the schedule. Example for Release #0001: Version 1: login, logout, password management Epics: 1 Sprints: 3 Total Story Points: 48 Version 2: purchase history Version 3: saving preferences
Risk Management	Capital Programming Guide	Risk Management refers to a systematic process of identifying, analyzing, and responding to risk. It includes maximizing the probability and consequences of positive events and minimizing the probability and consequences of adverse events to overall objectives. Risk management should be conducted throughout the entire life cycle of the program. http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/capital_programming_guide.pdf - Page 16
Risk Management Plan	Capital Programming Guide	Risk Management Plan refers to a documented and approved plan developed at the onset of the Investment and maintained throughout that specifies the risk management process. http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/capital_programming_guide.pdf - Page 16
"Shadow IT" or "Hidden IT"	OMB Memo M-15-14 https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf	Refers to spending on IT that is not fully transparent to the Agency CIO and/or IT resources included as a portion of a program that is not primarily of an "information technology" purpose but delivers IT capabilities or contains IT resources. For example, a grants program that contains a portion of its spending on equipment, systems, or services that provide IT capabilities for administering or delivering the grants.
Shared Service Provider	IT Budget - Capital Planning Guidance	This term refers to the provider of a technical solution and/or service that supports the business of multiple Agencies using a shared architecture. For Multi-Agency services, this is the Managing Partner of the Investment.

Term	Source Document	Definition
Shared Services	Federal IT Shared Services Strategy, May 2, 2012	This term refers to services that are provided by one Federal organization to other Federal organizations that are outside of the provider's organizational boundaries. Shared services may be Intra-Agency or Inter-Agency. There are three categories of shared services in the Federal Government: commodity IT, support, and mission services. • Commodity IT – including IT infrastructure and Enterprise IT services. • Support Services –capabilities that support common business functions performed by nearly all Federal organizations. These include functional areas such as budgeting, financial, human resources, asset, and property and acquisition management. Shared Commodity IT and Support Services are considered to be IT; associated costs must be included/reported as part of the IT Portfolio. • Mission Services – These are core purpose and functional capabilities of the Federal Government; such as disaster response, food safety, national defense, and employment services.
Software as a Service (SaaS) Cloud Computing	NIST Special Publication 800-145 -The NIST Definition of Cloud Computing	The capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based e-mail), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings (see NIST Special Publication 800-145 -The NIST Definition of Cloud Computing http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf).
TechStat Accountability Review	OMB Memo M-10-31	This term refers to a face-to-face, evidence-based review of an IT program with Bureau/Agency leadership and OMB as appropriate. TechStat sessions enable the Federal Government to turn around, halt, or terminate IT Investments that do not produce dividends for the American people. More detail regarding the TechStat process is described in the TechStat Training Deck (see https://cio.gov/deliver/techstat)http://www.whitehouse.gov/sites/default/files/omb/memoranda/2010/m10-31.pdf - Page 2).
Telecommunications	44 U.S.C. § 3542; OMB Circular A-130; OMB Circular A-11 (2010)	Includes telecommunications that are organized, procured and managed and/or operated by the Agency. Services may be provided for elements such as voice (voicemail, legacy voice service, and VoIP), data communications through the Wide Area Network (WAN)/Local Area Network (LAN) and associated access/transport options, Trusted Internet Connection (TIC), non-desktop Audio and Video Teleconference (VTC), and associated communications infrastructure elements (e.g., Structured Cabling Costs).

Term	Source Document	Definition
		• Voice Network/Services are (WASP/WITS, Legacy Analogue/Digital Voice, Voice Mail, Conference Bridge, automated operator services, and VoIP). • Wide Area Network (WAN) is a private, public or hybrid geographically dispersed network. • Local Area Network (LAN) is a private, public, or hybrid local area network. • Trusted Internet Connection (TIC) infrastructures, which provide a layer of consolidation and security for internet facing traffic. • Video Teleconferencing (VTC) is a collaborative meeting communications method. Only shared (non-desktop) locations should be included under telecommunications unless the desktop instance is a part of a specialized VTC used for remote or ad hoc shared connectivity. Typically utilizes PRI, IP, ISDN or Ethernet for connectivity. • Labor Costs including - FTE, Contract Support, Managed Services, and Other elements. Excludes cellular equipment, devices or services which are included in Mobile Devices.
Unique Investment Identifier (UII)	OMB Memo M-11-33	UII refers to a persistent numeric code applied to an Investment that allows the identification and tracking of an Investment across multiple FYs of an Agency's IT portfolio. The UII is composed of a three-digit Agency code concatenated with a nine-digit unique Investment number generated by the Agency. Some nine-digit numbers are reserved for OMB to assign and may not be assigned by Agencies, as controlled by the restrictions described in the section on "Variable Information." http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf - Page 14
User Stories	Forthcoming Agile Development Guidance	This term refers to high level requirements written by the project stakeholders or customers. These requirements are prioritized and further developed during sprints and determined acceptable by product owner or manager and stakeholders or customers.
Web Hosting, Infrastructure, and Content	OMB Circular A-11 (2010)	The following describes Infrastructure, and Content Management, Web Hosting: • IT Infrastructure Maintenance involves the planning, design, and maintenance of an IT Infrastructure to effectively support automated needs (e.g., platforms, networks, servers, printers). • Content Management includes capabilities to manage the storage, maintenance and retrieval of documents and information of a system or website. • Web Hosting refers capabilities to manage and provide availability to a web site or application, often bound to a Service Level Agreement (SLA). • Where appropriate, overlapping dollars should be entered in Mainframes and Servers only.

Appendix D. IT Security Capability Definitions

NIST Framework Function	Capability	Definition
Identify	Application Management	The practice of managing endpoint applications, including operating systems, to insure that deprecated, security vulnerable applications are known to all, they are detected if used, their execution is controlled/blocked by application whitelists, and ultimately, that common approved applications are resilient even to unknown exploits via advanced execution control techniques that interdict the cybersecurity attack chain.
Identify	Asset Management	The practice of tracking all known hardware assets of the enterprise, including manual, partially automated, fully automated, and continuous updates to the hardware attributable or connected to enterprise networks. Asset information includes machine type models, basic configurations, serial numbers, asset tags, user assignment and so forth. Full configuration control and update is part of configuration management.
Identify	Mobile Endpoint Management	The practice of managing mobile endpoints – from user provisioning, usage restrictions, geotagged security, applications allowed (mobile app management) – from cradle to grave. From a security standpoint, also maintaining standards for connection/communication with the enterprise network (e.g., e-mail, virtual desktop, other types of direct connection to enterprise systems).
Identify	Software Refreshment	The practice of managing enterprise systems, including operating systems and components of custom-developed systems, to insure that deprecated, security vulnerable software are known to all, they are detected if used, their execution is controlled/blocked by application whitelists, and ultimately, that common approved applications are resilient even to unknown exploits via advanced execution control techniques that interdict the cybersecurity attack chain.
Identify	Federal Government Outreach	Public-private partnerships, to include partners outside the Federal Government such as the Defense Industrial Base, owners of critical infrastructure, universities and other academia, and state and local governments. This also includes identifying, assessing, and mitigating cyber risks to mission essential functions in the nation's key critical infrastructures (previously "Public-Private Partnerships: Risk Management").
Identify	International Diplomacy	To include the costs of working with other governments to further cooperation on cybersecurity, including the development of cooperative activities for improving cybersecurity, international cooperation to investigate cyber incidents, safeguards for privacy, commercial transactions, and agreements on cybersecurity activities.
Identify	Standards Development and Propagation	Cybersecurity is becoming more standards-based to further improve automation, interoperability, and efficiency. NIST has the lead to develop standards, coordinate, and support Agencies.
Identify	Advisory Committee Activities	Statutorily defined advisory councils such as the Critical Infrastructure Partnership Advisory Council and the National Security Telecommunications Advisory Committee.
Identify	Other Identify Capabilities	To include other cybersecurity costs associated with the Identify function that have not been accounted for in other capability areas, including for management. Agencies must specify the activities attributed to this capability category and the spending associated with each activity. Agency spending in Other Identify Capabilities should not

NIST Framework Function	Capability	Definition
		exceed $10 million. If Agency spending for Other Identify Capabilities exceeds $10 million, Agencies should break the Investment into smaller individual components and describe them in greater detail.
Detect	Audit and Event Logging	The practice of maintaining full logs of all system activity, both internal and weblogs of externally-focused applications. System logs should be maintained and monitored by the developer teams and the associated systems security office. Beginning with web-facing systems, logs should be aggregated and ultimately fed into an enterprise security warehouse to assist in understanding security events that may have impacted the system in question.
Detect	Command & Control (CNC) Interdiction	The practice of blocking outbound traffic that is initiated by external, unapproved command & control type requests by an external CNC host. Can be as simple as URL blacklisting to more sophisticated DNS sinkholing and advanced CNC interdiction techniques.
Detect	Intrusion Detection	The practice of monitoring system activity through examining system traffic – both inbound and outbound – to match known intrusion patterns with the traffic, based on threat signatures provided by a vendor or developed internally.
Detect	Malware Analysis	The practice of analyzing a particular instance of malware to understand its behavior and what it is attempting to accomplish. This can be done through direct code analysis, out of band testing, creating a virtual sandbox for testing, or in-line, automated sandboxing, which may divert the malware, test it, then strip it out of network traffic or e-mail.
Detect	Malware Remediation	The practice of remediating the impacts of a particular instance of malware to return the system, application or e-mail to normal, non-threatening behavior. This can be done through restoration points; malware quarantine & deletion out of band; out of band payload removal, or in-line, automated content detonation/payload removal; and advanced execution control, which blocks payload execution at the process level in common applications.
Detect	Traffic Scanning	The practice of scanning all network traffic to identify, understand, and visualize traffic flow; capture, examine, and potentially block individual packets; and perform deep inspection – including encrypted traffic – to identify threats.
Detect	Anti-Phishing	The practice of implementing technologies and processes and that reduce the risk of malware introduced through e-mail and social engineering. This includes anti-phishing and -spam filters; analyzing incoming e-mail traffic using sender authentication, reputation filters, embedded content detection, and suspicious attachments; and utilizing end user authentication protocols on outgoing e-mail traffic to allow recipients to verify the originator.
Detect	Data Loss Prevention (DLP)	DLP is the practice of discovering sensitive content and blocking its exfiltration from the control of the enterprise. DLP systems are principally concerned with the data exiting a perimeter gateway, including emails, instant messages and Web 2.0 applications; however, this can be extended to copying of sensitive data to other media such as thumb drive, inappropriate collection and storage on a user endpoint, or printing of sensitive data.
Detect	Intrusion Prevention	The practice of intrusion prevention involves blocking and reporting suspicious activity on the enterprise perimeter or network. These can be security threats or policy violations. Intrusion prevention can include

NIST Framework Function	Capability	Definition
		dropping of malicious packets, blocking/filtering a specific URL, and so forth.
Detect	Threat Intelligence & Information Sharing	The practice of analyzing malware and determining its source, developing threat signatures, and sharing of the information within the security enterprise as well as to the larger security community.
Detect	Other Detect Capabilities	To include other cybersecurity costs associated with the Detect function that have not been accounted for in other capability areas, including for management. Agencies must specify the activities attributed to this capability category and the spending associated with each activity. Agency spending in Other Detect Capabilities should not exceed $10 million. If Agency spending for Other Detect Capabilities exceeds $10 million, Agencies should break the Investment into smaller, individual components and describe them in greater detail.
Protect	Configuration Management	Configuration management is the discipline and processes that to keep track of how hardware, operating systems, software versions and updates that are installed are deployed as part of the enterprise computing infrastructure. From a security standpoint, using unauthorized configurations is a negative and changes to configurations may be indicators of compromise that should be blocked from access until remedied.
Protect	Data Safeguarding – Data At Rest	Safeguarding data at rest involves strong data encryption. This begins with individual encrypted files, progressing to device encryption, data set encryption, etc. Ultimately, it can include data destruction to prevent compromise, including such concepts as remote data wiping and ephemeral data.
Protect	Data Safeguarding – Data in Motion	Safeguarding data in motion requires encryption as well, starting with methods of encrypted file transfer, encrypted emails, and progressing through transport layer security/SSL to virtual private networks to highly secure individual data networks.
Protect	Data Visibility	The practice of preventing casual insider threats to data, including timed lock screens on endpoints; data masking/obfuscation for high security data being accessed by developers/non-privileged users; surveying privileged user activity, including keystroke, videotaping, etc.; network detection of anomalous end-user behavior; and creating an end user culture of security which recognizes and reports potential insider threats.
Protect	Internet Access Management	The practice of managing how the enterprise connects to the public Internet, including ad hoc connections (dial-up, private lines, etc.), though self-managing of central gateways, to using the federal TIC and Managed Trusted Internet Protocol Service (MTIPS) services.
Protect	Vulnerability Analysis	Assessing the vulnerability of an enterprise by multiple means of vulnerability scanning and penetration testing, including automated PenTesting, formal Red Team Exercise, and continuous Red Team hacking to identify remaining vulnerabilities.
Protect	Vulnerability Management	Assessing the vulnerability of a particular system by a variety of techniques, including review of the system logs for exploitable errors, formal system vulnerability testing, automated testing and scanning, and ultimately leading to a security-by-design development approach.
Protect	Security Training	The practice of providing or otherwise ensuring users complete appropriate Cybersecurity Awareness and Training (CSAT). This includes conducting phishing exercises and role-specific training for users with significant security capabilities.

NIST Framework Function	Capability	Definition
Protect	Credentialing	Credentialing is a system by which identification cards or other tokens are used to authenticate a person and transmit skills, qualifications, and other attributes associated with that identity. This includes requiring authentication to access data/data systems; utilizing a physical token (e.g., ID badge) that reflects a particular level of assurance (LOA) required for access to a physical or logical enterprise enclave; verifying and maintaining the verification of a particular end-user's identity; federating the identities/access/authorities granted; and confirming the identity of a potential user before being allowed access to the physical or logical enclaves of the enterprise.
Protect	Authorization and Least Privilege	Least privilege is the principle that only the minimum necessary rights should be assigned to a subject and should be in effect for the shortest duration necessary. This includes managing the particular usage rights an authorized user has on a device or system; utilizing mechanisms by which a previously authenticated users are allowed to perform actions such as using a particular system within the enterprise; and ensuring authorization after access involves the user roles assigned and the access privileges this extends to data systems.
Protect	Cloud Services	The practice of acquiring cloud services and applications and ensuring they meet adequate security expectations. This includes assessing potential cloud services for alignment with established FedRAMP security baselines; acquiring tools to enhance the security of cloud-based applications; and the granting of ATOs to cloud service providers.
Protect	Counterintelligence	Information gathered and activities conducted to protect against cyber espionage, other intelligence activities, or sabotage conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities.
Protect	Research & Development	R&D related to cybersecurity and information assurance to protect computer-based systems from actions that compromise or threaten to compromise the authentication, availability, integrity, or confidentiality of these systems and/or the information they contain.
Protect	Other Protect Capabilities	To include other cybersecurity costs associated with the Protect function that have not been accounted for in other capability areas, including for management. Agencies must specify the activities attributed to this capability category and the spending associated with each activity. Agency spending in Other Protect Capabilities should not exceed $10 million. If Agency spending for Other Protect Capabilities exceeds $10 million, Agencies should break the Investment into smaller, individual components and describe them in greater detail.
Respond	Incident Management & Response	Case management – recording, ticketing, tracking, reporting, resolution – of a security incident; Security Operations Center (SOC) operators.
Respond	Federal Incident Response Centers	Government focal points for dealing with computer-related incidents affecting federal civilian Agencies. The centers provide a means for federal civilian Agencies to work together to handle security incidents, share related information, and solve common security problems.
Respond	Prosecution and Investigation of Cyber Intrusions	This includes the process of gathering evidence, attributing criminal acts to specific individuals, and pursuing criminal charges or civil actions against cyber perpetrators. This also includes actions associated with the investigation or prosecution of a criminal violation taken to reduce the extent or consequence of an adverse event affecting information systems, the information residing therein, or supported infrastructure (Previously Law Enforcement: Incident Response).

NIST Framework Function	Capability	Definition
Respond	Other Respond Capabilities	To include other cybersecurity costs associated with the Respond function that have not been accounted for in other capability areas, including for management. Agencies must specify the activities attributed to this capability category and the spending associated with each activity. Agency spending in Other Respond Capabilities should not exceed $10 million. If Agency spending for Other Respond Capabilities exceeds $10 million, Agencies should break the Investment into smaller, individual components and describe them in greater detail.
Recover	Disaster Recovery	Disaster recovery is the practice of returning a system or systems to operating capability by using back-up and restore techniques, duplicate "continuity of operations (COOP) sites", cloud-based restoration, or full cloud-based COOP operations.
Recover	Incident Notification	The practice of providing public/internal notifications to potentially impacted persons following cybersecurity incidents involving the possible loss of personally identifiable information (PII) and offering remediation for those adversely affected. This includes assessing potential impact to the public or internal populations; issuing public/internal notifications following an incident; tracking the issuance of notifications; and the acquisition and use of credit monitoring and credit repair services.
Recover	Other Recover Capabilities	To include other cybersecurity costs associated with the Recover function that have not been accounted for in other capability areas, including for management. Agencies must specify the activities attributed to this capability category and the spending associated with each activity. Agency spending in Other Recover Capabilities should not exceed $10 million. If Agency spending for Other Recover Capabilities exceeds $10 million, Agencies should break the Investment into smaller, individual components and describe them in greater detail.