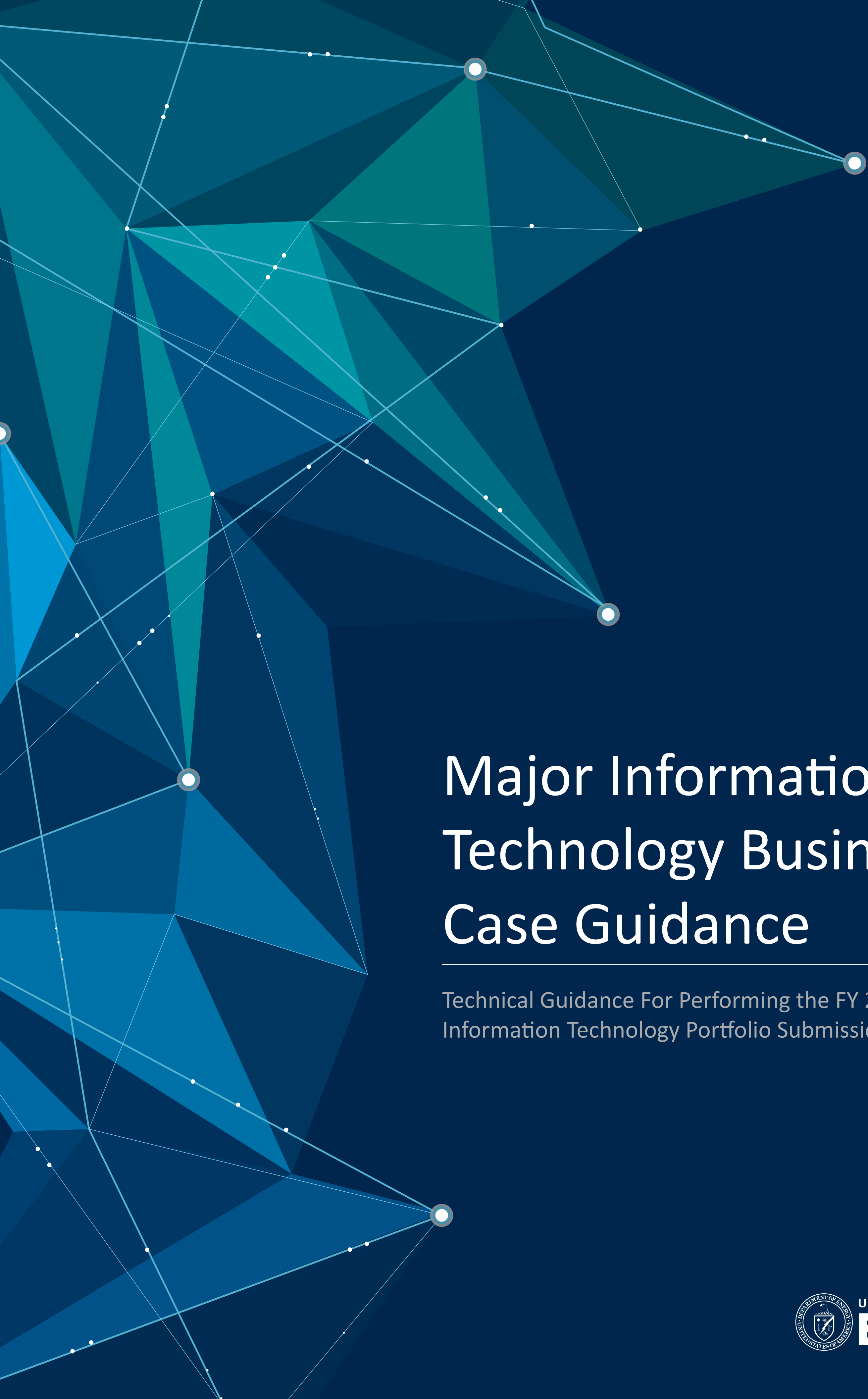


Major Information Technology Business Case Guidance

Technical Guidance For Performing the FY 2018 Information Technology Portfolio Submission

U.S. DEPARTMENT OF
ENERGY

Table of Contents

1 OMB MAJOR IT BUSINESS CASE

1.1 Major IT Business Case Defined

While the purpose of the Major IT Business Case remains the same, sections and/or content may change from year to year. This guidance is based on the Office of Management and Budget (OMB) Budget Year (BY) 2018 Major IT Business Case draft guidance and is subject to change.

OMB's Major IT Business Case guidance describes the justification, planning and implementation of an individual capital asset included in the agency IT investment portfolio and serves as a key artifact of the agency's Enterprise Architecture (EA) and IT Capital Planning Investment Control (CPIC) processes.

The Major IT Business Case is made up of two parts; 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. This business case helps align IT investments with strategic and performance goals, and ultimately provide value to the public by making investment and management information more transparent.

A major IT investment is a system and/or project (or a combination thereof) requiring special management attention because the investment:

- Has a cumulative steady state or mixed life cycle funding of $25 million or more across the Prior Year (PY), the Current Year (CY), and the Budget Year (BY);
- Is an OMB directed portfolio IT investment (Managing Partners for Government-wide E-Gov and Line of Business Investments are required to submit Major IT Business Cases unless they get a waiver from OMB. Refer to Appendix A for a list of Managing Partners);
- Is a managed designated shared service identified by the Unified Shared Service Management (USSM) within the General Services Administration (GSA) (Refer to Appendix for a list of Managing Partners);
- Is for the management of an IT Security and Compliance program;
- Requires special management attention because of its importance to the mission or function of the agency;
    1. Has significant program or policy implication;
    2. Has high executive visibility;
    3. Has high development, operating, or maintenance costs;
    4. Is funded through other than direct appropriations.

Investments not considered 'major' are classified as 'non-major.' A non-major investment is not required to complete the Major IT Investment Business Case, however investment managers should be aware of these requirements, as a non-major investment could be upgraded to a major investment if certain criteria are met.

NOTE: If the Major IT Investment is a High Performance Computer (HPC), please contact the DOE.CPICmailbox@hq.doe.gov for an alternate reporting template and instructions.

1.2 CIO Evaluation

All Major IT investments require a CIO evaluation score to be reported to the IT Dashboard. The CIO Evaluation is a numeric evaluation (1-5) that reflects the CIO’s best judgement of the current level of risk of the investment in terms of its ability to accomplish its goals. The evaluation is informed by the following factors:

CIO Evaluation Factors

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. ▪ Investment Team or Contracting Officer Representatives receives key reports, such as earned value, current status, and risk logs. ▪ Investment Team or Contracting Officer Representatives 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.

Each Major IT Investment will be evaluated by DOE periodically throughout the year. Every new Major IT Investment will get an initial CIO Evaluation as a preliminary evaluation for a planning investment.

2 Investment Documents in the Major IT Business Case Submission

The following documents are used in the decision-making process for selecting IT investments and are required 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 or mixed life cycle systems);
- Post implementation review results (investment level or project-specific); and,
- Documentation of investment re-baseline management approval(s)
- Documentation/Justification of an investment's elimination by: funding, consolidation, reorganization, or split.

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

Major IT investment managers are required to develop, maintain, and submit artifacts to the OCIO. Provide updated versions (including date of last update) to the OCIO a) when significant changes are made, b) within 30 days of its presentation to an Agency's governance board review (e.g. IRB/CIO review), or c) as available throughout the investment's lifecycle. New Major Investments should have these documents ready for review by the end of the month following the submission of the Final FY 2018 President's Budget Major IT Business Cases.

Templates for the required documents outlined above are located on the eCPIC Resource Library.

3 Major IT Business Case Sections to Complete

When completing the Major IT Business Case, investment owners should only fill out the sections that pertain to the individual investment. All major investments should complete the Major IT Business Case: Sections A, B, C and D.

For the Major IT Business Case Detail, all major investments should ensure Section A: General Information is complete. Development/Maintenance/Enhancements (D/M/E) and Maintenance investments should also complete Section B: Project Execution Data. Operational investments should omit Section B and complete Section C: Operational Data.

The following table demonstrates the specific sections of the Major IT Business Case and Major IT Business Case Detail to be completed based on the type of investment.

Sections of the Major IT Business Case and Detail to be Completed	D/M/E, Maintenance	Operations	Existing IT Security Major Investments	New IT Security Investments
Major IT Business Case: IT Capital Asset Overview and Justification				
Section A: General Information	x	x	x	x
Section B: Investment Detail	x	x	x	
Section C: Life Cycle Costs	x	x	x	x
Section D: Acquisition/Contract Strategy	x	x	x	x
Section E: Systems Inventory *(if Part 2 only)*	x	x		
Section F: Costs and Capabilities			x	x
Major IT Business Case Detail				
Section A: General Information	x	x	x	
Section B: Project Plan and Execution Data	x		x	
Section C: Operational Data		x	x	

NOTE: Mixed Lifecycle (DME & O&M) investments will need to complete all sections of the Major IT Business Case Detail.

Due to OMB's Major IT Business Case and Detail template changes, the Life Cycle Costs table and the Project and Activity tables may not match as they have in prior years. Please refer to the Performance Plan and Measurement Report section for further explanation.

Refer to the Appendix for OMB's list of Common Definitions for the IT Budget Submission and Integrated Data Collection (IDC). Additional budget terms and definitions are included in the Glossary in OMB Circular A-11, Appendix J, "Principles of Budgeting for Capital Asset Acquisitions."

Note: Investment and Project teams should not modify the structure or OMB IDs in eCPIC. These are used by the OCIO and OMB and should not be modified. If updates are required please contact DOE.CPICmailbox@hq.doe.gov.

4 MAJOR IT BUSINESS CASE

This section provides guidance to investment owners on how to complete the reporting requirements for Major IT Investments. This guidance provides instruction on completing these sections in eCPIC. Some of the field instruction and layout will differ from the official OMB IT Capital Planning Guidance.

4.1 Section A: General Information

If the fields for the Agency IT Investment Portfolio are up to date for BY 2018, then this section needs only be reviewed for accuracy.

Bureau (drop-down)

Select the appropriate DOE Bureau for the investment:

- National Nuclear Security Administration
- Environmental and Other Defense Activities (EM, LM, EHSS)
- Energy Programs (EE, EIA, FE, NE, OE, SC)
- Power Marketing Administrations (SEPA, SWPA, WAPA)
- Departmental Administration (GC, HG, IG, IM, CF, HR, MA, PA)
- Inter-Agency Projects
- Department Level or Agency-wide Activity

Change in Status Identifier (drop-down)

Select the identifier that correctly describes the investment's status for this budget submission, relative to the status in the previous budget cycle.

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:

- PSOs should confirm the selected status is for the current BY submitted (e.g., if the investment was reported as "New" during the BY17 submission, it should be reported as "No change in status" in the BY18 submission.)

- PSOs should also confirm that investment UIIs have not changed except for investments that selected 3, 4, 5, or 10.

Agency Description of Change in Investment Status (255 characters)

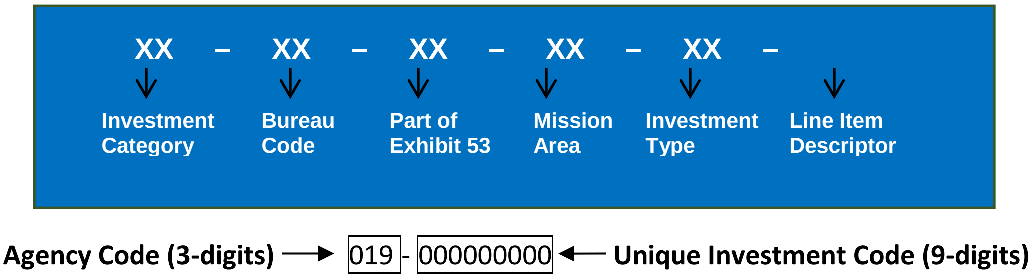
Mandatory field used when an indicator has been chosen for “Change in Investment Status” to provide more description of the rationale for the change. This field must end in a period (.).

Unique Investment Identifier

All new and existing investments are assigned a 12 digit number called a Unique Investment Identifier (UII). Each investment has a UII for identification and tracking purposes. The UII is made up of two parts: a 3-digit identifier that represents the Agency code and a 9-digit unique investment code that is generated by eCPIC when the investment is created. The “019” Agency Code indicates all Department of Energy investments.

Previous UII

Unique code reported in the previous BY Agency IT Portfolio Summary submission to OMB allowing cross-walk and historical analysis crossing FYs for tracking purposes. To indicate consolidations/splits/reorganizations, agencies can provide more than one entry and separate UIIs with commas. The Previous UII value is managed by the eCPIC Help Desk and is therefore read-only in eCPIC. PSOs should contact the eCPIC Help Desk with questions regarding the Previous UII.



Shared Services Category (drop-down)

If this investment provides or leverages a shared service, please select the appropriate identifier below (If the investment does not include shared services, then select “00”):

- 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: Share Service Providers (SSP) (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.

Shared Services identifier (free text)

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 D, 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-99999XXXX.

Part of Agency IT Portfolio Summary (drop-down)

Select the appropriate part based on the nature of the Investment. The details of each part are described above:

- 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 Information Technology

Standard IT Infrastructure and Management Category (drop-down)

Select the sub-category of Investments identified as Part 3: IT Investments for IT Infrastructure, IT Security, and IT Management. Investments for IT Security programs should use the IT Security & Compliance category (Category 02). Investments for CIO functions previously reported in Part 3 should use the IT Management category (Category 03). All other Investments should use Not Applicable (Category 01).

1. Not Applicable
2. IT Security & Compliance
3. IT Management

Type of Investment (drop-down)

Select the appropriate Investment Type based on the following criteria:

1. **Major IT Investment**

   DOE Criteria: OMB directed portfolio IT investments; Requires special management attention because of its importance to the mission or function of the agency; Significant program or policy implication; High executive visibility; High development, operating, or maintenance costs; or Funded through other than direct appropriations; Cumulative steady state or mixed life cycle funding of $25 million or more across PY, CY, and BY. (Every major investment identified on the Agency IT Portfolio Summary must have an approved Major IT Business Case).

2. **Non-major IT Investment**

   DOE Criteria: (Classify investment as "non-major" if it doesn't qualify as major investment as defined in the above criteria.)

3. **IT Migration Investment**

   Represents a portion of a larger asset and for which there is an existing business case for the overall asset. Description of the IT investment should indicate the UII of the major asset investment of the managing partner.

4. **Partner Agency Funding Contribution**

   Represents resources provided to a partner Agency for a joint effort by more than one agency. It is used to identify investments where the business case for the major IT investment is reported in another Agency's IT Investment Portfolio Summary. Description of the IT investment should indicate the UII of the major asset investment of the managing partner.

National Security Systems Identifier (drop-down)

Indicate whether or not the investment includes a National Security System

1. Non-National Security System Investment
2. National Security System Investment

Mission Delivery and Management Support Area (drop-down)

Select the mission delivery and management support area for the Investment:

- 01=Financial Management
- 11=National Nuclear Security Administration (NNSA)
- 12=Energy Efficiency & Renewable Energy (EE)
- 13=Energy Information Administration (EIA)
- 15=Environmental Management (EM)
- 16=Fossil Energy (FE)
- 17=Other Corporate Management (IM, CF, HR, MA and other DOE Staff Offices)
- 18=Nuclear Energy (NE)
- 21=Science (SC)
- 23=Power Marketing Administrations (WAPA, SWPA, and SEPA)
- 24=Environmental Health, Safety, and Security (EHSS)
- 25=Enterprise Assessments (EA)
- 31=Legacy Management (LM)
- 32=Electronic Delivery and Energy Reliability (OE)
- 99=Inter-Agency Projects

OMB Short Description

This is a short public-facing description for each investment explaining its purpose and what program(s) it supports, including the value to the public. It should be understandable to someone who is not an expert of the agency. If the investment is part of a multi-agency initiative or part of another business case the description should state this information and refer to the UII of the appropriate business case. This description is displayed on the Federal IT Dashboard and must end in a period (.) when entered in eCPIC.

4.2 Section B: Investment Detail

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.

- No change for BY18. 2500 character limit.
- Clearly describe the primary intent of this investment. What are the primary goals, objectives, and mission functions that the investment will support? Explain why it is important for this investment to be funded and/or include an assessment of the program impact if this investment is not fully funded. Include current or anticipated quantitative and/or qualitative benefits.
- Ensure all information is up-to-date in this response and consistent with other sections of the Major IT Business Case. For example, if specific investment details are updated in other sections of the Major IT Business Case, and are mentioned in the summary section, be sure to update the specific details in the summary as well.

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.

- No change for BY18. Open table for providing multiple codes.
- Refer to Appendix B for a list of all DOE Priority Goal and Strategic Objective codes.

Briefly describe the Investment's return on Investment, including benefits (internal and external to the government), and outcomes achieved or planned.

- Minor wording change for BY18 to include investment outcomes. 2500 character limit.
- Describe the investment's return on investment and expected benefits. Whenever possible, describe the return in quantifiable terms.

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.

- **Updated field requirements for BY18.** 2500 character limit.
- The old table format for describing specific requirements for the investment is replaced by an open text field. As with the table, URLs associated with the requirements should be provided in the response. Please note that each URL should be separated by a comma and space.

Identify the foremost program supported by this Investment

- No change for BY18.
- Refer to Appendix C for a list of current DOE programs and select the appropriate response. For investments that do not have a single primary program (e.g. Enterprise Solutions), enter 000-000.

If this Investment eliminates or reduces another major or non-major IT Investment(s), please list the Investment(s) and their status as eliminated or reduced.

- No change for BY18. Open table for listing multiple reduced or eliminated investments.

- 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.

Does the investment include a shared service (Intra- or Inter-Agency—current and/or planned)?

- No change for BY18. Yes/No option.

Are all systems funded by this investment PIV-enabled systems, per HSPD-12 and OMB M-11-11?

- No change for BY18. Yes/No option.

Provide any public facing URLs associated with this Investment, including APIs (if applicable). List as many URLs as apply.

- **Updated requirements for BY18.** Open table for listing multiple URLs.
- The old questions pertaining to the nature of the URL have been removed. New requirement only asks investments to list the URLs.

Investment Level Project Manager Contact Information and Qualifications.

- **New fields for BY18.**
- Provide the Name, Email Address, and Certification Qualifications of the investment-level project manager. The qualifications are listed as a drop-down menu with the following options:

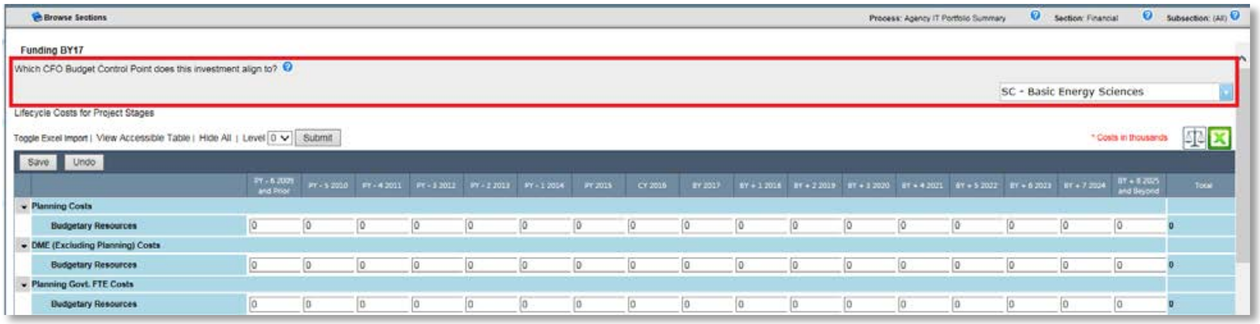
    1. FAC-P/PM(DAWIA-3) – Senior
    2. FAC-P/PM(DAWIA-2) – Mid-Level
    3. FAC-P/PM(DAWIA-1) – Entry Level
    4. Other certification with 4 or more years of PM experience (within the last five years)
    5. Other certification with between 2 and 4 years of PM experience (within the last five years)
    6. Other certification with less than two years of PM experience (within the last five years)
    7. No certification, but with 4 or more years of PM experience (within the last five years)
    8. No certification, but with between 2 and 4 years of PM experience (within the last five years)
    9. No certification, but with less than two years of PM experience (within the last five years)

4.3 Section C: Life Cycle Costs

This section consists of the tables necessary for populating the funding columns on the Agency IT Investment Portfolio Summary. These tables are also used for reporting Government Full Time Equivalents (FTE).

Chief Financial Officer (CFO) Budget Control Point

This DOE required field has been incorporated into the IT Portfolio Summary in order to identify the investments budget control point provided by the Office of the Chief Financial Officer (OCFO). The selection made should align with the CFO FY 2018 IT Budget Request exercise.



Browse Sections

Process: Agency IT Portfolio Summary | Section: Financial | Subsection: (All)

Funding BY17

Which CFO Budget Control Point does this investment align to?

SC - Basic Energy Sciences

Lifecycle Costs for Project Stages

Toggle Excel Import | View Accessible Table | Hide All | Level 0 Submit
Save
Undo

* Costs in thousands

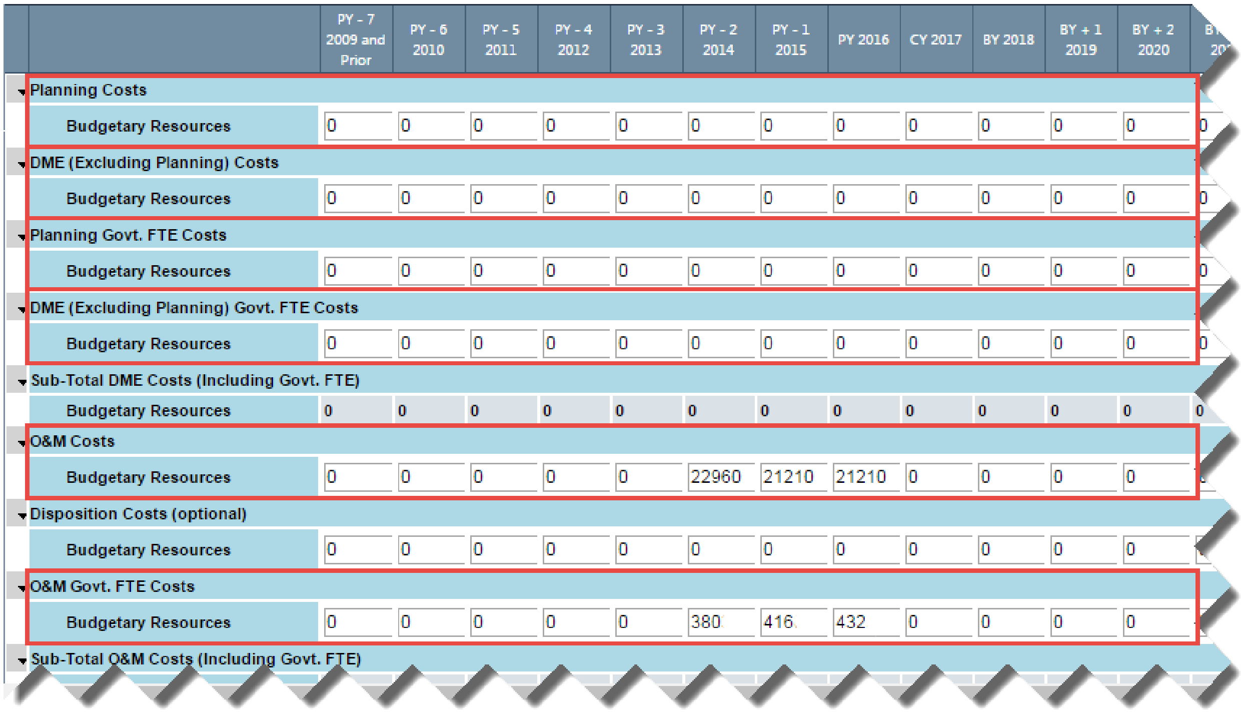
	PY - 6 2009 and Prior	PY - 5 2010	PY - 4 2011	PY - 3 2012	PY - 2 2013	PY - 1 2014	PY 2015	CY 2016	BY 2017	BY + 1 2018	BY + 2 2019	BY + 3 2020	BY + 4 2021	BY + 5 2022	BY + 6 2023	BY + 7 2024	BY + 8 2025 and Beyond	Total
Planning Costs																		
Budgetary Resources	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DME (Excluding Planning) Costs																		
Budgetary Resources	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Planning Govt. FTE Costs																		
Budgetary Resources	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Exhibit 1: CFO Budget Control Points in eCPIC

Life Cycle Costs Table

This table is used to track the full cost of an investment from planning through retirement. Investments should break-out Development/Modernization/Enhancement (DME) and Operations & Maintenance (O&M) funding requests by PY, CY, and BY. Report amounts in thousands ($k) when entering in eCPIC for all fiscal years. For example: $18,000 = 18 in eCPIC; or $1,500,000 = 1500 in eCPIC. Costs should be entered into the following categories as applicable:

- Planning
- Planning Govt. FTE Costs
- DME (Excluding Planning)
- DME (Excluding Planning) Govt. FTE Costs
- Operations and Maintenance
- Operations and Maintenance Govt. FTE Costs



	PY - 7 2009 and Prior	PY - 6 2010	PY - 5 2011	PY - 4 2012	PY - 3 2013	PY - 2 2014	PY - 1 2015	PY 2016	CY 2017	BY 2018	BY + 1 2019	BY + 2 2020	BY 20
Planning Costs													
Budgetary Resources	0	0	0	0	0	0	0	0	0	0	0	0	0
DME (Excluding Planning) Costs													
Budgetary Resources	0	0	0	0	0	0	0	0	0	0	0	0	0
Planning Govt. FTE Costs													
Budgetary Resources	0	0	0	0	0	0	0	0	0	0	0	0	0
DME (Excluding Planning) Govt. FTE Costs													
Budgetary Resources	0	0	0	0	0	0	0	0	0	0	0	0	0
Sub-Total DME Costs (Including Govt. FTE)													
Budgetary Resources	0	0	0	0	0	0	0	0	0	0	0	0	0
O&M Costs													
Budgetary Resources	0	0	0	0	0	22960	21210	21210	0	0	0	0	
Disposition Costs (optional)													
Budgetary Resources	0	0	0	0	0	0	0	0	0	0	0	0	
O&M Govt. FTE Costs													
Budgetary Resources	0	0	0	0	0	380	416	432	0	0	0	0	
Sub-Total O&M Costs (Including Govt. FTE)													

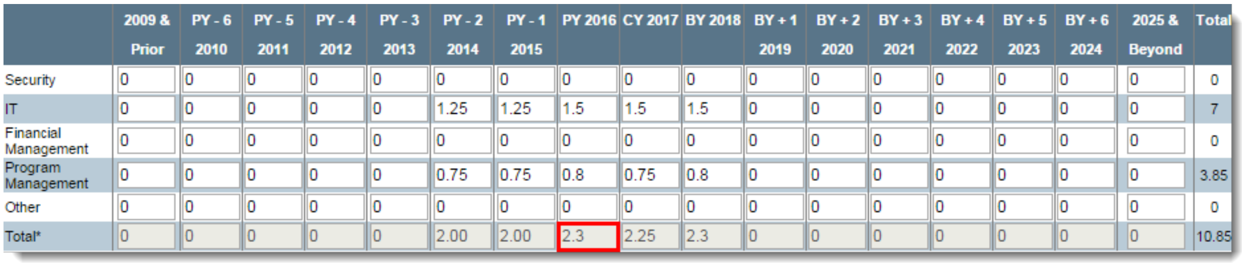
Exhibit 2: Life Cycle Costs Table in eCPIC

For detailed definition of DME and O&M, please refer to the eCPIC Resource Library for the Integrated Data Collection (IDC) common definition of terms (see Appendix A).

Government FTEs

This is the number of government FTEs included in the PY, CY, and BY funding and the total PY, CY, and BY investment cost represented by the number of government FTE. This applies to all investments, both major and non-major. If an FTE's costs are included in the investment costs for PY, CY, or BY, the FTE or portion of the FTE should be reported, regardless of the FTE's role in the investment (technical, managerial, functional, or governance). PSOs should verify FTEs are reported consistently. Government FTE costs are captured in the Life Cycle Costs Table. **Exhibit 1** (above) highlights the "Govt. FTE Costs" rows in that table.

Exhibit 3 displays the FTE table in eCPIC. FTE counts in this table are entered as decimals to reflect a portion of an FTE's time being devoted to work under this investment. For example, the "2.3" represents two FTEs, plus 30% of another FTE's time. PSOs should verify the FTE costs in the Life Cycle Cost Table align with the FTE count in the FTE table.



	2009 & Prior	PY - 6 2010	PY - 5 2011	PY - 4 2012	PY - 3 2013	PY - 2 2014	PY - 1 2015	PY 2016	CY 2017	BY 2018	BY + 1 2019	BY + 2 2020	BY + 3 2021	BY + 4 2022	BY + 5 2023	BY + 6 2024	2025 & Beyond	Total
Security	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IT	0	0	0	0	0	1.25	1.25	1.5	1.5	1.5	0	0	0	0	0	0	0	7
Financial Management	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Program Management	0	0	0	0	0	0.75	0.75	0.8	0.75	0.8	0	0	0	0	0	0	0	3.85
Other	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Total*	0	0	0	0	0	2.00	2.00	2.3	2.25	2.3	0	0	0	0	0	0	0	10.85

Exhibit 2: FTE Table in eCPIC

To determine the average costs of FTEs for the investment, take the total FTE costs from the Life Cycle Costs Table (**Exhibit 1**) and divide by the Total FTEs in the FTE Table (**Exhibit 3**). For the example taken from **Exhibits 1 & 3** above, the average cost per FTE in PY 2016 is $165,217 ($380k/2.3 FTEs).

In which year did or will this investment begin?

- No change for BY18.

In which year will this Investment reach the end of its estimated useful life?

- No change for BY18.

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.

- No change for BY18.

Funding Sources

For each investment, provide the funding source(s) and total budgetary resources that contribute to the investment (**Figure 2**). An agency should add as many funding source line items as are appropriate for the investment. For each reported year, the sum of all funding source(s) amounts for an investment must equal its total investment costs as reported in the Life Cycle Costs table (above). Report amounts in thousands ($k) when entering in eCPIC for all fiscal years. For example: $18,000 = 18 in eCPIC; or $1,500,000 = 1500 in eCPIC.

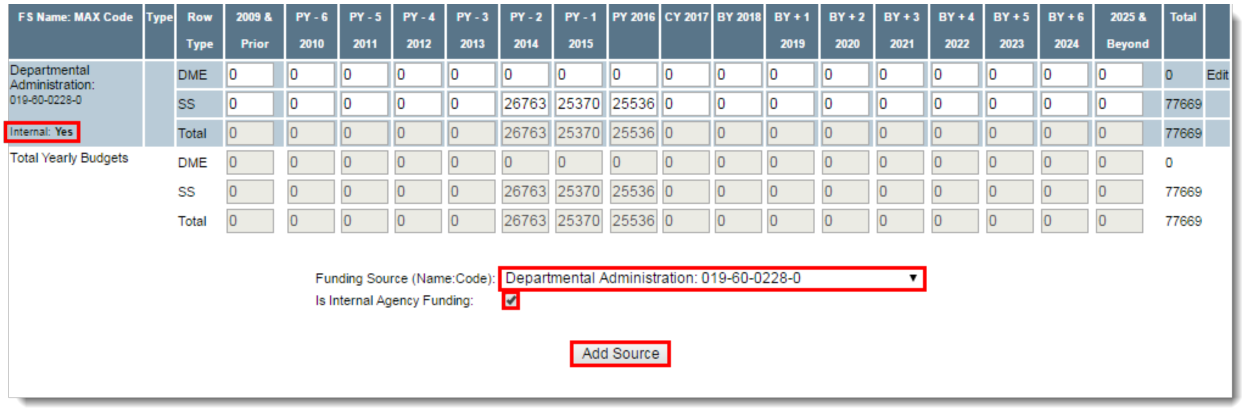
- <u>Agency Funding</u>

  Reports the agency's budgetary resources for a given investment for PY (2016), CY (2017), and BY (2018). Agency Funding can be identified by designating a funding source as "Internal = Yes".

- <u>Contributions (PY) /Expected Contributions (CY and BY)</u>

  Includes both monetary contributions and fees for services provided by partner agencies to managing partners or shared service providers of a multi-agency collaboration. Contributions should only apply to multi-agency collaboration. Actual contributions should be reported for PY (2016), as well as expected contributions for CY (2017) and BY (2018). Contributions can be identified by designating a funding source as "Internal = No".

Below is the Funding Source table in eCPIC.



FS Name: MAX Code	Type	Row	2009 &	PY - 6	PY - 5	PY - 4	PY - 3	PY - 2	PY - 1	PY 2016	CY 2017	BY 2018	BY + 1	BY + 2	BY + 3	BY + 4	BY + 5	BY + 6	2025 &	Total	
		Type	Prior	2010	2011	2012	2013	2014	2015				2019	2020	2021	2022	2023	2024	Beyond		
Departmental Administration: 019-60-0228-0		DME	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Edit
		SS	0	0	0	0	0	26763	25370	25536	0	0	0	0	0	0	0	0	0	77669	
Internal: Yes		Total	0	0	0	0	0	26763	25370	25536	0	0	0	0	0	0	0	0	0	77669	
Total Yearly Budgets		DME	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
		SS	0	0	0	0	0	26763	25370	25536	0	0	0	0	0	0	0	0	0	77669	
		Total	0	0	0	0	0	26763	25370	25536	0	0	0	0	0	0	0	0	0	77669	

Funding Source (Name:Code): Departmental Administration: 019-60-0228-0 ▼

Is Internal Agency Funding: ☑

Exhibit 3: Funding Sources Table in eCPIC

4.4 Section D: Acquisition / Contract Strategy

The overall structure of this section has changed for BY18. In previous years, all contract information was reported in a single table for awarded contracts only. For BY18, OMB created two tables to capture both the awarded contracts and the planned acquisitions.

Existing Contracts

- **Updated field for BY18.** Open table for capturing all awarded contracts.
- Provide in this table information for all awarded prime contracts (or task orders) for the investment. <u>Do not include</u> sub-award details, Inter-Agency Agreements (IAA), or Memoranda of Understanding (MOU) in this table. Utilize the <u>Federal Procurement Data System (FPDS)</u> to confirm certain data points in the table (noted below).
- For each entry within the Existing Contracts table, provide the following information:

  1. Procurement Instrument Identifier (PIID)

     - PIID can be found as data element 1A on FPDS. Please work with your procurement representative if you have any questions regarding the contracts you are reporting.

2. Referenced PIID

   - This field was called the IDV PIID in BY17. It can be found as data element 1C on FPDS.

3. Modular Approaches/Contracting *[Yes/No]*

   - Do acquisition planning, award, and management actions apply the principles and strategies described in "Contracting Guidance to Support Modular Development"?

4. Agile Development *[Yes/No]*

   - Does this contract employ agile development techniques?

5. EVM Required? *[Yes/No]*

   - Will EVM be required as part of this contract?

6. Purpose of needing this procurement *[500 Character limit]*

   - 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.

7. 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

8. Information Security Clause *[Yes/No]*

   - Does this contract include information security clauses regarding the use, storage or other processing of data?

Do any of the existing or planned contracts/task orders ensure accessibility and/or are fully compliant with Section 508 standards?

- **New field for BY18.** Single-select box with Yes/No options available.
- Use this box to indicate whether or not all contracts within this investment are compliant with the requirements of Section 508.

Acquisition Strategy

- **New field for BY18.** Open table for capturing all planned acquisitions.
- Provide in this table all planned procurements for this investment, to include pre-award phase, active solicitations, and planned IAA or MOU.
- For each entry within the Acquisition Strategy table, provide the following information:

1. Description of the Planned Contract Support *[1000 character limit]*

   - 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.

2. Anticipated Award Date or IAA/MOU Signature *[MM/DD/YYYY]*
3. Length of Planned Period of Support *[20 character limit]*
   - What is the expected time frame for which this support is needed?
   - Express in terms of base time frame and options. For example: 90 days, 180 days, 1 year, 2 years, 5 years, etc.
4. Anticipated Value *[$k]*
   - The anticipated value of the required support in terms of total cost.
5. Modular Approaches/Contracting *[Yes/No]*
   - Do acquisition planning, award, and management actions apply the principles and strategies described in "Contracting Guidance to Support Modular Development"?
6. Agile Development *[Yes/No]*
   - Will this procurement employ agile development techniques?
7. EVM Required? *[Yes/No]*
   - Will EVM be required as part of this procurement?
8. Potential Sources *[500 Character limit]*
   - 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? For example: CIOSP3, Schedule 70, etc.
9. Provider Engagement *[1000 Character limit]*
   - What strategies are being considered to reach out to innovative provider has been performance? For example: Market engagement, RFIs, industry days, etc.
10. IT Lease *[Yes/No]*
    - Will this planned procurement contain a lease (as defined by OMB Circular A-11 Appendix-B)?
11. PIID of Replaced Contract(s)
    - 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.
    - PIID is data element 1A on FPDS.
12. Referenced PIID of Replaced Contract(s)
    - 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.
    - Referenced PIID is data element 1C on FPDS.

4.5 Section E: Systems Inventory *(Administrative Services and Support Systems Only)*

This section will only be filled out for investments that are categorized as Part 2: IT Investments for Administrative Services and Support Systems (See Part of Agency IT Portfolio Summary field in section 4.1 above). For each Part 2 investment, complete the following table:

Systems Inventory

- **New requirement for BY18.** Open table for capturing all systems included as part of this investment.
- For each system included in this investment, provide the following information:
    1. System Name *[250 character limit]*
    2. Initial Operating Year *[YYYY]*
    3. Last Major Tech Refresh Date *[MM/DD/YYYY]*
    4. End of Contract Support *[MM/DD/YYYY]*
    5. Average Number of Users Per Month *[10 character limit]*

4.6 Section F: IT Security Costs and Capabilities *(IT Security & Compliance Investments Only)*

This section will only be completed for investments that are listed as “IT Security & Compliance” standard investments under the Standard IT Infrastructure and Management Category field (See Agency IT Investment Portfolio, Column 7, Code 02).

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.

Each record in the table below should represent a unique security capability that corresponds to a NIST Framework Category (see Appendix B). 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.

Costs and Capabilities

- **New requirement for BY18.** Open table to capture all IT Security Capabilities funded through the investment.
- For each IT Security Capability funded by this investment, provide the following information:
    1. NIST Framework Category – See Appendix C for alignment between NIST Framework Categories and Capabilities.
        - Select the appropriate NIST Category aligned to the IT Security Capability.
            - Identify

- Protect
- Detect
- Respond
- Recover

2. Capability – See Appendix C for descriptions of each capability within the NIST Framework.
   - Select the capability associated with the IT security spending in the PY, CY and/or BY years.
   - To facilitate more complete reporting, each NIST Framework Category includes a “Other” capability category Agencies may utilize for cybersecurity costs for which they would not have otherwise accounted. 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.
3. Purpose/Outcome *[1000 character limit]*
   - Describe the purpose and intended outcomes from money spent on the reported capability. Also describe any expected fluctuations in spending across the 3 years.
4. Budget Account
   - List the OMB Budget Account Code(s) that fund the capability.
5. PY 2016 Total
   - Enter the total PY 2016 spending on the capability.
6. CY 2017 Total
   - Enter the total CY 2017 planned spending on the capability.
7. BY 2018 Total
   - Enter the total BY 2018 planned spending on the capability.

5 Major IT Business Case Detail

5.1 Section A: General Information

All major IT investments, except new IT security and compliance major investments, are required to fill out Section A of the Major IT Business Case Detail.

Investment Name

This data is pulled from the Agency IT Investment Portfolio Summary.

Investment UII

This data is pulled from the Agency IT Investment Portfolio Summary.

Investment Risk

- **Updated requirement for BY18.** Open table for capturing all investment-level risks.

- Enter all active risks at the investment level and provide the following risk assessment information for each:

    1. Risk Name *[500 character limit]*

        - Include here a short description that identifies the risk, the cause of the risk and the effect that the risk may have on the Investment.

    2. Risk Category

        - Select the OMB Risk Category that best describes the nature of the risk.
            - Schedule
            - Initial costs
            - Life cycle costs
            - Technical obsolescence
            - Feasibility
            - Reliability of systems
            - Dependencies and interoperability between this Investment and others
            - Surety (asset protection) considerations
            - Risk of creating a monopoly for future procurements
            - Capability of Agency to manage the Investment
            - Overall risk of Investment failure
            - Organizational and change management
            - Business
            - Data/info
            - Technology
            - Strategic
            - Security
            - Privacy
            - Project resources

    3. Risk Probability *[Low/Medium/High]*

        - Select the likelihood of a negative impact for the risk.

    4. Risk Impact *[Low/Medium/High]*

        - Select the appropriate level of negative effect should the event occur.

    5. Mitigation Plan *[500 character limit]*

        - Provide a short description of the plan that is in place to mitigate the negative impact of the risk.

- Major IT investments are required to submit a minimum of one investment risk.

- NOTE: For existing major IT investments, all open operational risks from BY17 will be migrated over into this table for BY18. Please review all existing risks to ensure they are still valid.

5.2 Section B: Project Plan and Execution Data

This section is used to report Development, Modernization, and Enhancement (DME) spending activities within the investment. This section should also be used to report maintenance projects (e.g. activities that may fall under O&M, but have specific a specific start date, end date, and tasks).

B. 1 Projects Table

- Minor change for BY18. Open table for capturing all projects underway within the investment.
- For each project, provide the following information:

1. Project ID *[10 character limit]*
    - Provide a unique identifier for the project. Use alphanumeric characters only.
2. Project Name *[250 character limit]*
    - Provide the name used by the Agency to refer specifically to this project.
3. Objectives/Expected Outcomes *[2500 character limit]*
    - Provide a description of the project’s functionality, capability, or goal.
4. Project Start Date *[MM/DD/YYYY]*
    - Date of actual start of in-progress projects or planned start of projects which have not yet begun (may be before current fiscal year or activities listed in the B.2.1 and/or B.2.2 tables).
5. Project Completion Date *[MM/DD/YYYY]*
    - 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 the B.2.1 and/or B.2.2 tables).
6. Project Life Cycle Cost *[numeric]*
    - Enter the total cost of all activities related to the project as described in OMB Circular A-131 (in thousands, $k).
7. System Development Life Cycle (SDLC) Methodology
    - Select the most appropriate option for the project.
        - Waterfall
        - Spiral
        - Iterative (Prototyping/Incremental)
        - Agile
        - Mixed
        - Other
        - Not Primarily a Software Development Project
8. Other SDLC? *[500 character limit]*
    - Provide a description of the SDLC methodology employed for any projects that selected “Other” in column 7.
9. Production Release Every 6 Months *[Yes, No, N/A]*
    - Select the frequency at which this project releases functional updates. N/A is only a valid option for projects that selected “Not Primarily a Software Development Project” in column 7.
10. Comment

    - If this project does not release usable functionality at least every six months, provide a rationale explaining why this is the case.
    - This field is required if “No” is selected in column 14.

11. When was the last date that a revised product wad deployed to production? *[MM/DD/YYYY]*
    - Provide the date that the most recent system changes were 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 if “Not Primarily a Software Development Project” is selected for column 7.

Project Activities

The following tables are used to report the planned and in-progress activities and tasks for the projects defined for the investment in the B.1 Projects Table (above). At a minimum, all projects with any activities that started in a previous FY (FY 2016 and earlier) and have not completed by the beginning of the CY (FY 2017) as well as projects and activities that are scheduled to start in the CY (FY 2017) and BY (FY 2018), including planning, DME, and maintenance projects. Include projects and activities commencing beyond the BY (FY 2018) as available.

In BY18, two tables are available for reporting these activities depending on the SDLC Methodology of the project.

B.2.1 Project Activities Table (Standard)

The B.2.1 Standard Project Activities Table is used to report activities in a more traditional, WBS-type format. Activities are grouped into a hierarchical structure that allows for multiple levels of complexity to report parent-child relationships between activities. Any project listed in the B.1 Projects Table can utilize the B.2.1 Table for reporting project activities.

- No change for BY18.

B.2.2 Project Activities Table (Agile)

The B.2.2 Agile Project Activities Table can be used to report activities for projects that selected “Agile” as their SDLC Methodology in the B.1 Projects Table. The fields in this table are catered to be more in line with agile methodologies, and therefore improve reporting accuracy.

Agile projects have the option to use this table in lieu of the B.2.1 Standard Project Activities Table. Within an investments, both tables can be utilized, but a single project cannot report activities to OMB using both tables (a single table must be chosen for each project).

- **New optional field for BY18.** Open data grid used to capture agile project activities.

  For each agile project activity, provide the following information:

1. Project ID *[10 character limit]*
    - Provide a unique identifier for the project. Use alphanumeric characters only.
2. Project Name
    - Select the project to which this activity aligns. Only “Agile” projects from the B.1 Project Table will appear in this drop-down.
3. Release Name
    - Provide a name for the release. If possible, this should align with the Product Backlog.
4. Release Number
    - Provide the number of the release. If possible, this should align with the Product Backlog.
5. Release Description
    - Provide a description of the release. Include a brief description of the updates planned to be completed in the release.
6. Start Date *[MM/DD/YYYY]*
    - Provide the Planned, Projected, and (if applicable) Actual Start Dates for the release.
7. Completion Date *[MM/DD/YYYY]*
    - Provide the Planned, Projected, and (if applicable) Actual Completion Dates for the release.
8. Total Cost *[in thousands, $k]*
    - Provide the Planned, Projected, and (if applicable) Actual Total Costs for the release.
9. Number of Planned Iterations (NPI)
    - Provide the number of planned iterations or sprints included in the release.
10. Number of Planned Epics (NPE)
    - Provide the number of planned Epics to be included in the release. Fractions of an Epic (denoted with decimals) are acceptable.
11. Number of Completed Epics (NCE)
    - Provide the number of completed Epics included in the final release. Fractions of an Epic (denoted with decimals) are acceptable.
12. Number of Completed Iterations (NCI)
    - Provide the number of completed iterations or sprints included in the final release.
13. Direct Technical Contributors (DTC)
    - Provide the number of direct technical contributors on the project.

14. Direct Personnel Contributors (DPC)

    - Provide the number of other staff contractors on the project.

5.3 Section C: Operational Data

Operational Analysis

- **New requirement for BY18**. Data chooser and free text area.
- Provide the date of the most recent operational analysis performed for this investment. This requirement applies to all investments with mixed lifecycle or operational components.
- In the free text are, provide a description of the results of the analysis.

C.1A Operational Performance Table

- No change for BY18. Open table for capturing the performance metrics that will be measured for this investment in BY18.
- For all investments with operational or mixed lifecycle components, a minimum of five operational performance metrics must be defined for measurement in FY 2017.
- All data will be displayed to the public on the ITDB. Ensure that all metrics provided are publicly releasable
- For each metric, provide the following information:

1. Metric ID *[Alphanumeric]*
    - Provide a unique identifier for the metric. This is defined by the investment manager, and is only required to be unique within the investment, not the Agency.
2. Metric Name [250 character limit]
    - Provide a name for the metric. This name is used to align actual results to this metric in eCPIC and is not included in submissions to the OMB IT Dashboard.
3. Metric Description [500 character limit]
    - Provide a description of what this metric is measuring. Describe the units used, any calculations used, and the definition of the population or universe that is being measured.
4. Unit of Measure
    - Indicate the units that will be used to report on this metric (e.g. number, percent, dollars, etc.).
5. Performance Measurement Category Mapping
    - Identify the measurement category for this metric. Select from the following
        - Customer Satisfaction (Results) *[One metric required minimum]*
        - Strategic and Business Results *[Three metrics required minimum]*
        - Financial Performance *[One metric required minimum]*
        - Innovation
6. Agency Baseline Capability *[numeric]*

  - Provide the quantitative value for the Department's capability to meet this metric prior to the start of this investment's life cycle.
    - For example, what would the actual result be for this metric if this investment and its supported systems/services did not exist at DOE?
  - Provide this number in the same units as the targets for 2016 and 2017.

7. Target for 2016 *[numeric]*
  - If this metric was measured for this investment in FY 2016, provide the target used last year. Do not include units when entering the target.

8. Target for 2017 *[numeric]*
  - Define the target for this metric for FY 2017. Do not include units when entering the target.

9. Measurement Condition
  - Provide the condition for which the actual results for the metric are considered "Met". In other words, will this metric be considered successful if my result is above the target or below?

10. Reporting Frequency
  - Provide the frequency at which actual results will be reported for the metric:
    - Monthly
    - Quarterly
    - Semi-Annual
    - Annual
  - At least one metric designated as a "Strategic and Business Result" metric must report at a Monthly frequency.
  - 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.

11. Agency Strategic Objective or Priority Goal
  - At a minimum, one metric designated as "Strategic and Business Results" must provide a Strategic Objective or Priority Goal code. The codes can be found in Appendix B.
  - At least one Strategic Objective or Priority Goal code listed in the table must align with the code provided as the response for the second question in the Major IT Business Case, Section B: Investment Details.

12. Is the Metric Retired?
  - For passed metrics that are no longer being reported on, please designate them as retired to close them out on the ITDB.

C.1B Operational Performance Actual Results Table

- No changes for BY18. Open table for capturing actual results reported for the metrics in the C.1A Table.

- At the defined frequency, enter actual results for each metric in the C.1A Table by filling out the following fields:
    1. Metric Name
        - Select the metric for which the actual result is being reported.
    2. Actual Result *[numeric]*
        - Provide the actual result. Do not enter units with the result.
    3. Date of Actual Result
        - Provide the date that the actual result was reported.
    4. Comment *[500 character limit]*
        - Provide a comment for any metric actual results that are not meeting their defined targets.

6 Data Submission Logistics

This section provides logistics for investment owners to submit their data to their PSOs for submissions to the OCIO for review and feedback.

In the chart below, each organization's senior IT manager who owns a portfolio of IT investments in eCPIC will be responsible for updating, reviewing and certifying via email to DOE CPIC mailbox that their organization's submission is complete for OCIO review. After the OCIO review, PSOs will be notified if the submission is satisfactory or if further modifications are necessary.

Due Date	Responsible Party	Action
7/1	OMB	OMB Circular A-11 & BY 2018 Capital Planning Guidance Published
7/13	OMB, OCIO	OMB/DOE Joint CPIC Workgroup Meeting
8/11	OCIO	Release of the DOE BY 2018 CPIC Technical Guidance for Agency IT Portfolio and Business Case Submissions
8/23	OCIO	BY 2018 Template Available in eCPIC (effective close of business)
8/31	Headquarters, eCPIC, Investment owners, and Portfolio owners	DOE Program Office Deadline for Submission of the following in eCPIC: (1) Preliminary/Draft BY 2018 IT Investment Portfolio and Agency Provisioned IT Services Spending Summary (Cloud Spending) (2) Provide the names of any new, upgraded or downgraded major IT investment(s) to DOE.CPICmailbox@hq.doe.gov
9/1 – 9/12	OCIO	OCIO reviews preliminary BY 2018 IT Investment Portfolio data and Agency Provisioned IT Services Spending Summary (Cloud Spending) and provides Performance Improvement Plan (PIP) feedback, where appropriate.

9/9	OCIO	Draft submission to the Office of Management and Budget (OMB) by the OCIO of the following: (1) IT Portfolio Summary (2) Budget Accounts Summary
9/19 – 9/22	OCIO	DOE Cyber Conference in Atlanta, GA.
9/23	Headquarters, eCPIC, Investment owners, and Portfolio owners	DOE Program Office Deadline for Submission of the following in eCPIC: (1) Final Updates to BY 2018 IT Investment Portfolio (2) Final Provisioned IT Services Spending Summary (3) Final Data Center Spending Summary
9/26 – 9/30	OCIO	eCPIC Lockdown & Portfolio Data Validation Period
9/30	OCIO	Final Submission to OMB by the OCIO of the following: (1) IT Portfolio Summary (2) Budget Accounts Summary (3) Provisioned IT Spending Summary (4) Data Center Spending Summary
10/12	Headquarters, eCPIC, Investment owners, and Portfolio owners	DOE Programs Submit Final Updates to Existing Major IT Investment Business Cases in eCPIC
10/13	OCIO	eCPIC Lockdown & Existing Major Business Case Data Validation Period
10/14	OCIO	Submission of Existing Major IT Investment Business Cases to OMB by the OCIO
11/10	Headquarters, eCPIC, Investment owners, and Portfolio owners	DOE Programs Submit Final New Major IT Investment Business Cases, including Security and Compliance Investments in eCPIC
11/14 – 11/18	OCIO	eCPIC Lockdown & Business Case Data Validation Period
11/18	OCIO	Submission of New Major IT Investment Business Cases to OMB by the OCIO

12/1	OCIO/OCFO	CIO/CFO "IT Resource Statement" Certification (*Pursuant Circular A-11, Sec. 51.3*) Uploaded to MAX Portal
TBD	OMB	Final FY 2018 President's Budget Submissions

7 How to Access or Add a Resource to an Investment or Portfolio

7.1 Investment Resources

eCPIC provides a **Resource Library** that allows users to access and download reference materials from anywhere in the application, including the Home Page.

The Resource Library includes three category types: General Resources, Investment Resources, and Portfolio Resources.

7.1.1.1 General Resources

General Resources are accessible to all users from the public-facing Resource Library. This is accessible from the eCPIC Home Page (prior to logging in) or from the Resource Library Module (after logging in).

To access the Resource Library Module:

1. Click on the **Resource Library** module in the Navigation Pane.

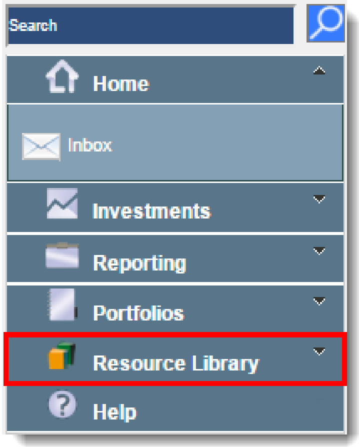
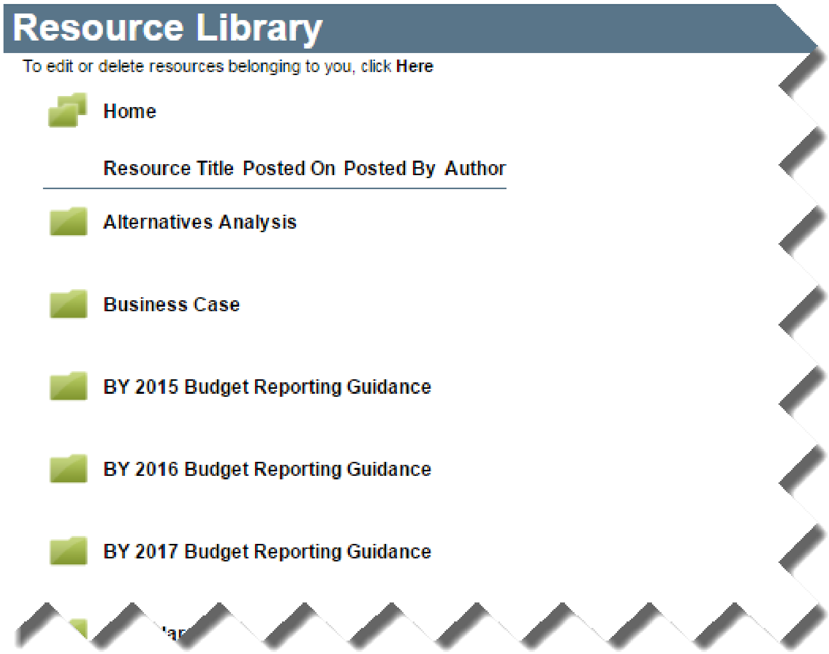


Exhibit 4: Resource Library Module Link

This will open the General Resource Library.



Resource Library

To edit or delete resources belonging to you, click Here

Alternatives Analysis

Business Case

BY 2015 Budget Reporting Guidance

BY 2016 Budget Reporting Guidance

BY 2017 Budget Reporting Guidance

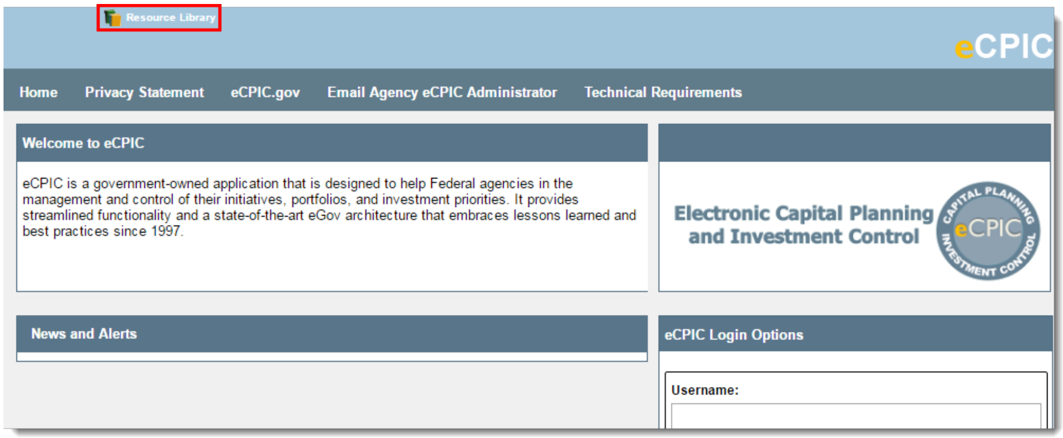
Exhibit 5: General Resource Library Home

2. Click on a folder to view the documents within that category, then click directly on the document name to open or download it on your computer.

To access the General Resource Library if you do not see the Resource Library link in the Navigation Pane:

1. Logout of eCPIC.

2. From the login screen, click on the Resource Library link at the top of the browser window.



Resource Library
eCPIC
Home
Privacy Statement
eCPIC.gov
Email Agency eCPIC Administrator
Technical Requirements

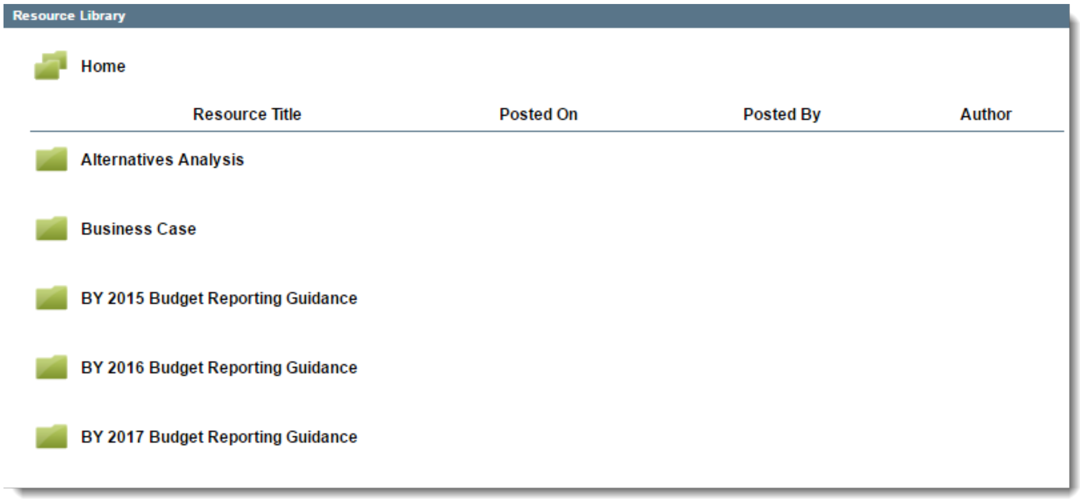
Welcome to eCPIC

eCPIC is a government-owned application that is designed to help Federal agencies in the management and control of their initiatives, portfolios, and investment priorities. It provides streamlined functionality and a state-of-the-art eGov architecture that embraces lessons learned and best practices since 1997.

Electronic Capital Planning and Investment Control
CAPITAL PLANNING eCPIC INVESTMENT CONTROL
News and Alerts
eCPIC Login Options
Username:

Exhibit 6: eCPIC Login Page With Resource Library Link Highlight

3. The General Resource Library will appear in a separate window.



Resource Library

Home

Resource Title	Posted On	Posted By	Author
Alternatives Analysis			
Business Case			
BY 2015 Budget Reporting Guidance			
BY 2016 Budget Reporting Guidance			
BY 2017 Budget Reporting Guidance			

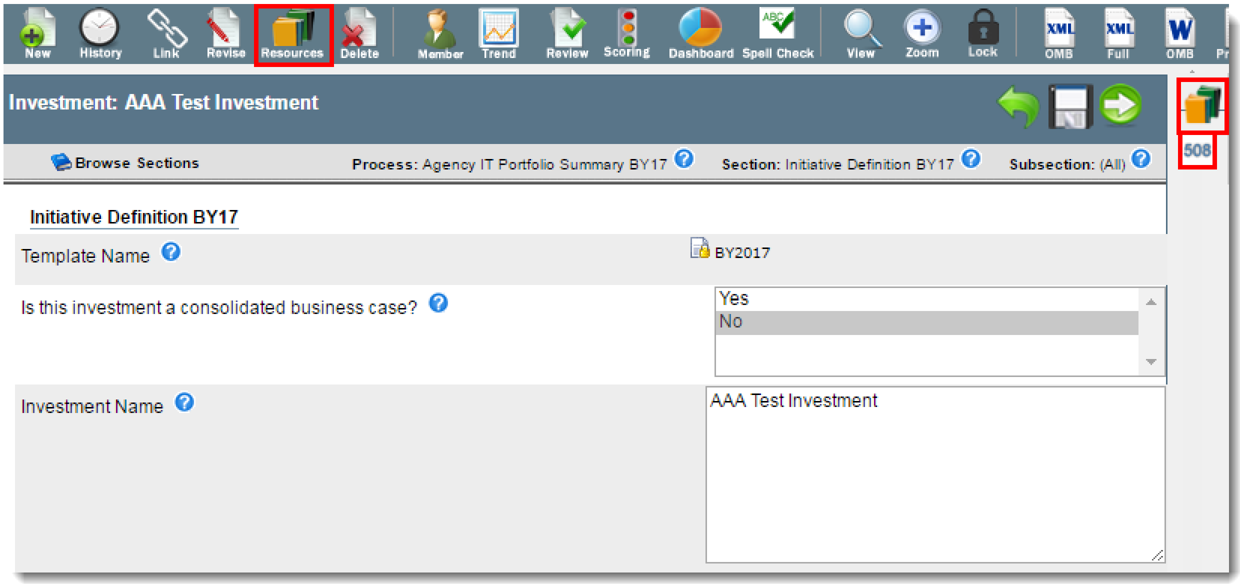
Exhibit 7: Public-Facing Resource Library Pop-Up Window

4. From this window, documents and folders can be accessed as described in the Resource Library Module steps.

7.1.1.2 Investment and Portfolio Resources

The Investment and Portfolio Resources are found in each respective module. From each module, access to the Resource Library can be toggled on or off. To toggle the Resource Library on:

1. Click on the **Toggle Resource List** icon (Resources) in the toolbar of either module. The Resource List icon ( ) will appear on the side of the investment. There will also be the (508) icon. **Exhibit 5** shows how this appears within an investment. **Exhibit 6** shows the same for a portfolio.



Investment: AAA Test Investment

Browse Sections | Process: Agency IT Portfolio Summary BY17 | Section: Initiative Definition BY17 | Subsection: (All)

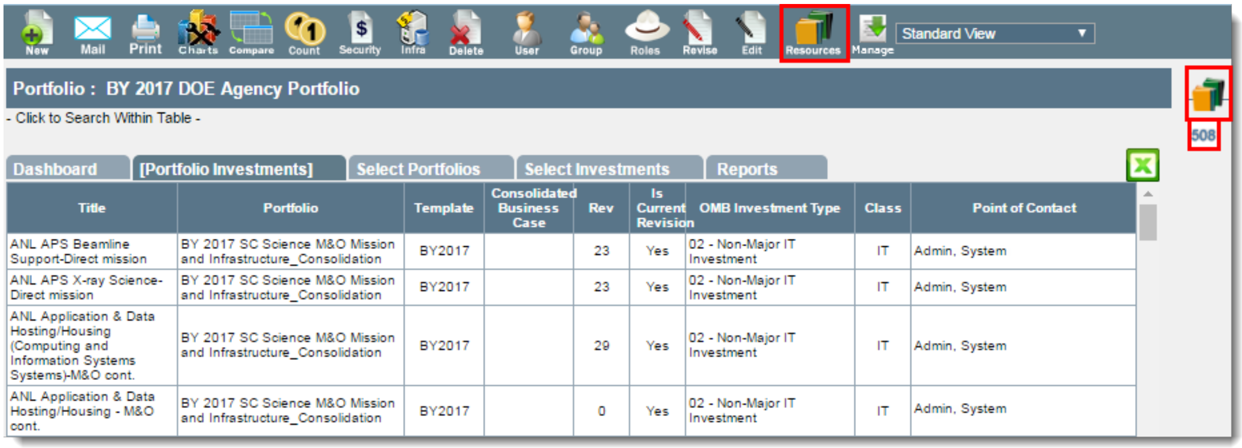
Initiative Definition BY17

Template Name: BY2017

Is this investment a consolidated business case? Yes [✓ No]

Investment Name: AAA Test Investment

Exhibit 8: Investment Resource Library



Portfolio : BY 2017 DOE Agency Portfolio

- Click to Search Within Table -

Title	Portfolio	Template	Consolidated Business Case	Rev	Is Current Revision	OMB Investment Type	Class	Point of Contact
ANL APS Beamline Support-Direct mission	BY 2017 SC Science M&O Mission and Infrastructure_Consolidation	BY2017		23	Yes	02 - Non-Major IT Investment	IT	Admin, System
ANL APS X-ray Science-Direct mission	BY 2017 SC Science M&O Mission and Infrastructure_Consolidation	BY2017		23	Yes	02 - Non-Major IT Investment	IT	Admin, System
ANL Application & Data Hosting/Housing (Computing and Information Systems Systems)-M&O cont.	BY 2017 SC Science M&O Mission and Infrastructure_Consolidation	BY2017		29	Yes	02 - Non-Major IT Investment	IT	Admin, System
ANL Application & Data Hosting/Housing - M&O cont.	BY 2017 SC Science M&O Mission and Infrastructure_Consolidation	BY2017		0	Yes	02 - Non-Major IT Investment	IT	Admin, System

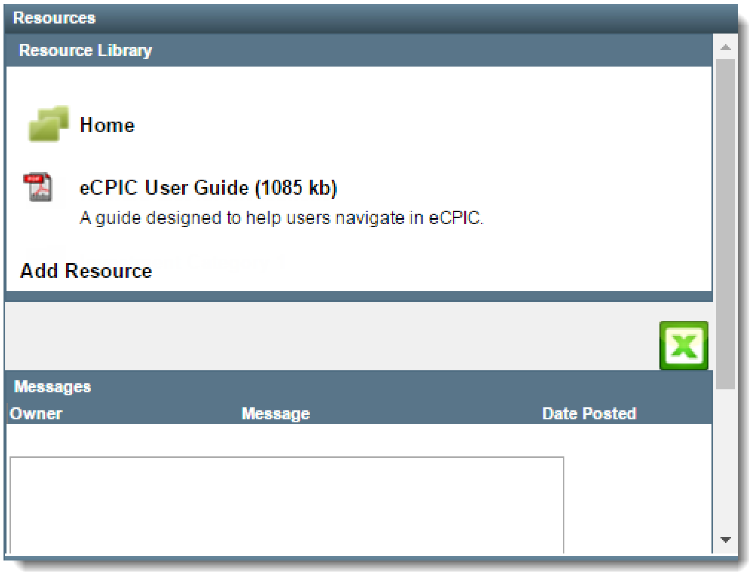
Exhibit 9: Portfolio Resource Library

7.2 Accessing Documents in the Resource Library

To access the data within an investment or portfolio, go to the appropriate module and select the investment or portfolio for which you want to access Resource Library documents:

1. Toggle the Resource Library on (see section 9.1).

2. Mouse over the resource library icon on the right hand side of the display window to show the Resource Library and Messages. The Resource Library window contains a list of Resources that relate specifically to the investment.



eCPIC User Guide (1085 kb)

A guide designed to help users navigate in eCPIC.

Owner	Message	Date Posted

Exhibit 10: Resource Library Window

3. Click on the name of the resource (**eCPIC User Guide** in **Exhibit 7**) to download the resource to the computer. *Note: If the resource is a link, the link will open in another browser window.*

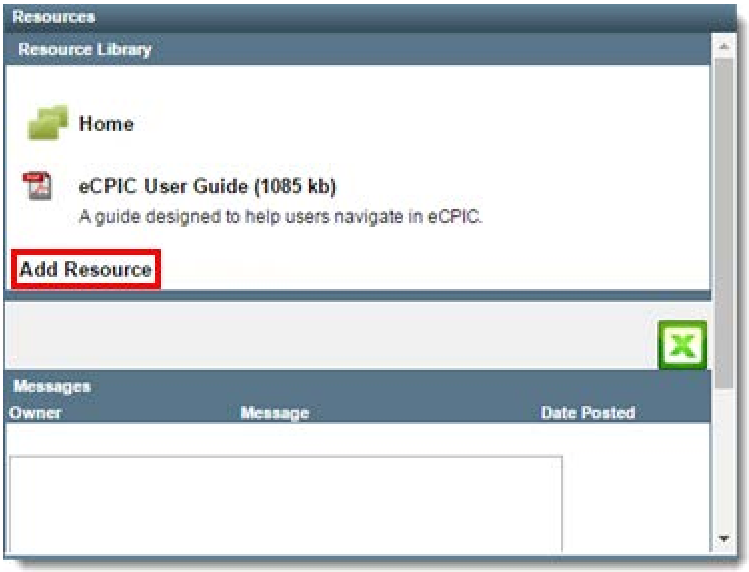
4. A dialog box will appear asking you to either **Save** or **Open** the file. Click **Save**.

7.3 Add an Investment or a Portfolio Resource

With the "Create" Right for the Resource Library, users will be able to add Resources to the Resource Library of an Investment and a Portfolio. To add documents into an investment or portfolio resource library:

1. Toggle the Resource Library on (see section 9.1).

2. Mouse over either icon to view the Resource Library and a Messages box to show the Resource Library and Messages.

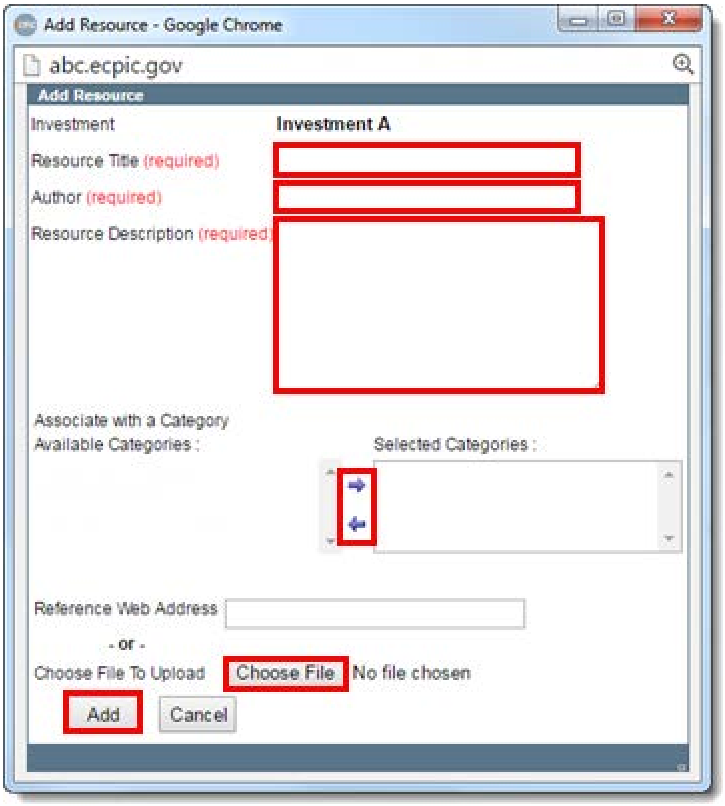


eCPIC User Guide (1085 kb)

A guide designed to help users navigate in eCPIC.

Exhibit 11: Highlight of the 'Add Resource' Button

3. In the Resource Library window, click **Add Resource**. The Add Resource form will appear:



Investment Investment A

Exhibit 12: Add Resource Form With Field Highlights

4. In the Add Resource form, enter the Title, Author, and Description.

5. If there are Resources Categories available, users will see them listed in the 'Available Category' box. Users can associate the Resource with a category by highlighting the specific category and clicking the ➡ arrow to move it to the 'Selected Category' box. To remove a category from the 'Selected Category', highlight the category and click on the ⬅ arrow to move it back in the 'Available Category' box.

Note: Holding 'Shift' while selecting categories will highlight multiple categories at one time in the order which they are listed. Holding 'Ctrl' while selecting names, will allow users to highlight a category and select other categories that may not be in order.

6. If adding a Web link, enter the address in the 'Reference Web Address' field.
   Note: Don't forget to add the http:// to the beginning of the link.

7. If adding a document, click **Choose File** and navigate to find the appropriate file.

8. After all information is complete, click Add. The Resource will now be associated with the investment or portfolio and any Category specified.

8 Appendix A – Unified Shared Service Management (USSM) Office Designated Shared Service List

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	1104
OCFO-NFC Shared Services	USDA	National Finance Center	NFC	Core HR, Payroll	1208

9 Appendix B – Agency Strategic Objectives and Priority Goal Codes

Department of Energy Agency Priority Goals

Agency Priority Goal	Code
Environmental Management and Nuclear Waste Disposal	90511
Modernize the nuclear stockpile	45442
Energy Policy	45482

High Performance Computing	45492
Manage DOE Capital Asset Projects	45502
National Laboratories	45512

Department of Energy Agency Strategic Objectives

Strategic Goal	Strategic Objective	Code
Science and Energy	Climate Action Plan	5192
Science and Energy	Energy Infrastructure	5202
Science and Energy	Scientific Discoveries	5222
Nuclear Security	Nuclear Deterrent	5242
Nuclear Security	Strengthen Key Science, Technology, and Engineering Capabilities and Modernize the National Security Infrastructure	5262
Nuclear Security	Reduce Global Nuclear Security Threats	5272
Nuclear Security	Provide Safe and Effective Integrated Nuclear Propulsion Systems for the U.S. Navy	5282
Management and Performance	Continue Cleanup of Radioactive and Chemical Waste	5342
Management and Performance	Manage assets in a Sustainable Manner that Supports the DOE Mission	5352
Management and Performance	Effectively Manage Projects, Financial Assistance Agreements, Contracts, and Contractor Performance	5362
Management and Performance	Operate the DOE Enterprise Safely, Securely, and Efficiently	5372
Management and Performance	Attract, Manage, Train, and Retain the Best Federal Workforce	5382

10 Appendix C – Agency Program Codes

Department of Energy Program Codes

Program Name	Program Code
Advanced Manufacturing Office (formerly Industrial Technologies)	**019-001**
Building Technologies	**019-002**
Vehicle Technologies	**019-003**
Weatherization and Intergovernmental Programs	**019-004**
Bioenergy Technologies (formerly Biomass and Biorefinery R&D)	**019-005**
Geothermal Technology	**019-006**
Hydrogen and Fuel Cell Technologies	**019-007**

Solar Energy	**019-008**
Water Power	**019-009**
Wind Energy	**019-010**
Federal Energy Management Program	**019-011**
Petroleum Reserves	**019-012**
Fossil Energy R&D	**019-013**
Nuclear Energy (NE)	**019-014**
Electricity Delivery and Energy Reliability (OE)	**019-015**
Bonneville Power Administration (BPA)	**019-016**
Southeastern Power Administration (SEPA)	**019-017**
Southwestern Power Administration (SWPA)	**019-018**
Western Area Power Administration (WAPA)	**019-019**
Loan Programs (LP)	**019-020**
Advanced Research Projects Agency-Energy (ARPA-E)	**019-021**
Energy Information Administration (EIA)	**019-022**
Advanced Scientific Computing Research	**019-023**
Basic Energy Sciences	**019-024**
Biological and Environmental Research	**019-025**
Fusion Energy Sciences	**019-026**
High Energy Physics	**019-027**
Nuclear Physics	**019-028**
Workforce Development for Teachers and Scientists	**019-029**
Directed Stockpile Work	**019-030**
Science Campaign	**019-031**
Engineering Campaign	**019-032**
Inertial Confinement Fusion Ignition and High Yield Campaign	**019-033**
Advanced Simulation and Computing Campaign	**019-034**
Readiness Campaign	**019-035**
Nuclear Programs	**019-036**
Secure Transportation Asset	**019-037**
Facilities and Infrastructure Recapitalization Program	**019-038**
Site Stewardship	**019-039**
Defense Nuclear Security	**019-040**
NNSA CIO Activities	**019-041**
Global Threat Reduction Initiative	**019-042**
International Material Protection and Cooperation	**019-043**
Fissile Materials Disposition	**019-044**
Nonproliferation and International Security	**019-045**
Defense Nuclear Nonproliferation Research and Development	**019-046**
Nuclear Counterterrorism Incident Response Program	**019-047**
Counterterrorism and Counterproliferation	**019-048**
Naval Reactors	**019-049**

NNSA Office of the Administrator	**019-050**
Environmental Management (EM)	**019-051**
Legacy Management (LM)	**019-052**
Departmental Administration: Support Offices/Corporate Management	**019-053**
(Primary Program Not Available)	**019-000**

11 Appendix D – OMB Common Definitions

Term	Source Document	Definition
Adequate Incremental Development	OMB Memo M-15-14	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	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/asset s/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.
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	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 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](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, 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. 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 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/as sets/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 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/mem oranda/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 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. • 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/mem oranda/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.
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 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.
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	OMB Circular A-127	This term refers to systems necessary to support financial management, including automated and

Systems		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/Busine ss 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 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	FEA Business Reference	Help Desk Services involves the operation of a

Support)	Model v 3.0	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 Publication800-145 -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/m emoranda/fy04/m04-25.pdf and FISMA, section 3542(b)(1)(A-C)
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_a130tra ns4, 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	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.
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	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 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."
IT Migration	IT Budget - Capital	This term refers to the migration costs associated

Investment	Planning Guidance	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 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	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- 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/asset s/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.
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 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 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.
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 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	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 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.
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	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.
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	NIST Special Publication	The capability provided to the consumer to use the

Service (SaaS) Cloud Computing	800- 145 -The NIST Definition of Cloud Computing	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 http://www.whitehouse.gov/sites/default/files/omb/memoranda/2010/m10-31.pdf - Page 2).
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.

12 APPENDIX E – NIST FRAMEWORK CATEGORIES AND CAPABILITIES

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 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 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.
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).
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.