GUIDANCE ON EXHIBIT 53—INFORMATION TECHNOLOGY AND E-GOVERNMENT

Table of Contents

Summary of Changes

Significantly updates Exhibit 53 requirements. In particular:

- Changes Unique Project Identifier to Unique Investment Identifier plus Variable Information.
- Updates special terms related to IT and E-Government (Section 53.4).
- Updates Exhibit 53B, "Agency IT Security Portfolio."
- Requires agencies to submit a draft FY 2013 Exhibit 53A&B to OMB by Aug. 31, 2011 and a final Exhibit 53A&B on September 12, 2011; for agencies on the IT Dashboard, draft and final exhibits must be submitted electronically to the IT Dashboard (Section 53.6).

53.1 Why must I report on information technology (IT) investments?

The information required allows the agency and the Office of Management and Budget (OMB) to review and evaluate each agency's IT spending and to compare IT spending across the Federal Government. Specifically the information helps the agency and OMB to:

- Provide a report on all IT investments for the agency as required by the Clinger-Cohen Act of 1996;
- Understand and compare the amount being spent on development of new capabilities (Development, Modernization and Enhancement – DME, which may appropriately be treated as capitalized costs), and operation and maintenance (O&M or Steady-State) for all agency IT investments;
- Identify and report IT security costs for all IT investments and for agency and bureau IT security programs as required by the Federal Information Security Management Act (FISMA);
- Identify and report on agency financial management systems.

Agencies must provide this information using the Agency IT Investment Portfolio (Exhibits 53A&B) reporting format. This information should be consistent with information required in Section 51 of OMB Circular A-11. In addition, as an output of your agency's internal IT capital planning and investment control process, your Budget justification for IT must provide results-oriented information in the context of the

agency's missions and operations, as expressed through the agency's enterprise architecture. Your Budget Justification, including the status and plans for information systems, should be consistent with your agency's submissions for Exhibit 300A&B submissions (see guidance on Exhibit 300A&B), regarding major IT Investments.

The investment's costs must include all Federal budgetary resources (direct appropriation, working capital fund, revolving funds, etc.). Budgetary resources are defined in Section 20 of OMB Circular A-11. Life cycle costs as maintained in agency IT capital planning systems should also be risk adjusted to include any risks addressed in the IT investment's business case and summarized in the IT Capital Asset Summary (Exhibit 300A). These investment costs must be formulated and reported to OMB, in order for OMB to meet the Clinger-Cohen Act's requirement which states that at the same time the President submits the Budget for a fiscal year to Congress under Section 1105(a) of title 31, United States Code, the Director shall submit to Congress a report on the net program performance benefits achieved as a result of major capital investments made by executive agencies in information systems and how the benefits relate to the accomplishment of the goals of the executive agencies.

53.2 What background information must I know?

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

- The Clinger-Cohen Act of 1996, which requires agencies to use a disciplined capital planning and investment control (CPIC) process to acquire, use, maintain and dispose of information technology in alignment with the Agency's enterprise architecture planning processes. OMB policy for management of Federal information resources is contained in Circular A–130, "Management of Federal Information Resources."

- The Government Performance and Results Act of 1993 (GPRA), which establishes the foundation for Budget decision-making to achieve strategic goals in order to meet agency mission objectives. Instructions for preparing strategic plans, annual performance plans, and annual program performance reports are provided in Part 6 of OMB Circular A-11 (see Section 220).

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

- The Federal Managers Financial Integrity Act of 1982 (FMFIA), Chief Financial Officers Act of 1990 (CFO Act) and Federal Financial Management Improvement Act of 1996, which require accountability of financial and program managers for financial results of actions taken, control over the Federal Government's financial resources, and protection of Federal assets. OMB policies and standards for developing, operating, evaluating, and reporting on financial management systems are contained in Circular A–127, Financial Management Systems, and OMB CircularA-11 Section 52.

- The Paperwork Reduction Act of 1995 (PRA), which requires agencies to perform their information resources management activities in an efficient, effective, and economical manner.

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

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

- The National Technology Transfer and Advancement Act (NTTAA) of 1995 (Public Law 104-113) and OMB Circular A-119 , which state that voluntary consensus standards are the preferred type of standards for Federal government use. When it would be inconsistent with law or otherwise impractical to use a voluntary consensus standard, agencies must submit a report describing the reason(s) for the agency's use of government-unique standards in lieu of voluntary consensus standards to the Office of Management and Budget (OMB) through the National Institute of Standards and Technology (NIST).

- The Federal Records Act, which requires agencies to establish standards and procedures to assure efficient and effective records management. The National Archives and Records Administration (NARA) issues policies and guidance for agencies to meet their records management goals and requirements. NARA also provides policies and guidance for planning and evaluating investments in electronic records management.

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

- The 25 Point Implementation Plan to Reform Federal Information Technology Management should inform agency, bureau and branch planning for the planning, development, management, operation and governance of Federal information technology.

Sustainable Computing statutes, executive orders and regulations:

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

- Executive Order 13423 —Strengthening Federal Environmental, Energy, and Transportation Management

- Federal Acquisition Regulations (FAR) including Subchapter B, Parts 5 through 12 and Part 23

- Federal Management Regulation (FMR) including Subchapters B and C

- Energy Independence and Security Act of 2007, including Sections 431 through 435 and 523 through 525

- Energy and Policy Act of 2005 including Sections 103, 104, 109 and 203

53.3 How do I ensure that IT investments are linked to and support agency strategic plans?

Each IT investment must clearly demonstrate that the investment is needed to help meet the agency's strategic goals and mission by demonstrating how the investment supports a business line or enterprise service performance goal as documented in a Segment of the Agency’s Enterprise Architecture. Agency IT

investment business cases (and other documents), the IT Capital Asset Summary (Exhibit 300A) and "Agency IT Investment Portfolio" (Exhibit 53A) demonstrate the agency's management of IT investments and how governance processes are used to plan, select, develop, implement and operate IT investments. Documents used to manage the planning, development, implementation and operation of IT investments, and that demonstrate the outcomes of agency, branch and bureau governance decisions should be maintained and be readily available if requested by OMB.

The individual agency's Exhibit 53A and Exhibit 300As are used to create an overall "Federal IT Investment Portfolio" published as part of the President's Budget. Agency and OMB portfolio reviews and Budget processes will ensure the selection of IT investments that support the strategy identified in this section.

Cloud First Policy (IT Reform)

Since December 2010, agencies have been required to institute a 'Cloud first' implementation approach for all IT investments; this new policy should be incorporated into the agency's IT strategic plan. The 'Cloud first' policy is intended to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments. As per the Federal Cloud Computing Strategy, agencies should be evaluating their technology sourcing plans to include consideration and application of cloud computing solutions as part of the budget process. Consistent with the Cloud First policy, agencies will modify their IT portfolios to fully take advantage of the benefits of cloud computing in order to maximize capacity utilization, improve IT flexibility and responsiveness, and minimize cost. When evaluating options for new IT deployments, OMB will require 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 lifecycle stage. Where appropriate, all agency cloud evaluations must include an assessment of cloud solutions approved by the Federal Risk and Authorization Management Program (FedRAMP) and leverage government-wide and enterprise cloud computing procurements.

The 25 Point Implementation Plan to Reform Federal Information Technology Management calls for agencies to shift to the 'Cloud First' Policy.

53.4 What special terms should I know?

Business Reference Model (BRM) is one of five reference models of the Federal Enterprise Architecture (FEA). It is a classification taxonomy used to describe business function and sub-function areas as well as related services that are performed within and between federal agencies and with external partners. IT investments are mapped to the BRM to identify opportunities for collaboration, shared services, and solution reuse. BRM function, sub-function and service component codes are found in the FEA Consolidated Reference Model at:
http://www.whitehouse.gov/sites/default/files/omb/assets/fea_docs/FEA_CRM_v23_Final_Oct_2007_Revised.pdf

Note: In April 2010, the BRM and the former "Service Component Reference Model" (SRM) were combined, with updated definitions to follow in early FY 2012 with the release of v2 of the FEA and updates to the Consolidated Reference Model. The acronym "SRM" with respect to the FEA now refers to the Security Reference Model. A six-digit BRM code is used in Exhibit 53 submissions for all IT investments.

Capital Planning and Investment Control (CPIC) means the same as capital programming and is a decision-making process for ensuring IT investments integrate strategic planning, budgeting, procurement, and the management of IT in support of agency missions and business needs. The term comes from the Clinger-Cohen Act of 1996 and generally is used in relationship to IT management issues.

Contributions (Expected Contributions) 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 collaborations.

FEA mapping codes captured in the Ex 53a are as follows. The first 3-digit code indicates the business area served by this investment (the 3-digit BRM sub-function code). The second 3-digit code indicates the services also associated with this investment (the service component code). Guidance on the codes for these mappings can be found at http://www.whitehouse.gov/omb/e-gov/fea/.

Federal Enterprise Architecture (FEA) is a business-based documentation and analysis framework for government-wide improvement. The FEA allows agencies to use 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) and six reference models areas that are designed to facilitate standardized analysis, reporting, and the identification of duplicative investments, gaps, and opportunities for collaboration within and across federal agencies. More information about the FEA and reference models is available at http://www.whitehouse.gov/sites/default/files/omb/assets/fea_docs/FY10_Ref_Model_Mapping_QuickGuide_Aug_2008_Revised1.pdf

Federal IT Dashboard is a website enabling federal agencies, industry, the general public and other stakeholders to view details including performance for federal information technology investments.

Federal Segment Architecture Methodology (FSAM) is to become the "Federal Solution Architecture Methodology" in October 2011 and will serve as a scalable and repeatable process for solution architecture at the application, system, segment, enterprise, sector, government-wide, national, and international levels of scope. Consistent use of the FSAM should result in more complete and consistent architecture products by helping architects engage system owners, program offices, and executive sponsors to deliver value-added plans for improved mission delivery. Specifically, FSAM includes guidance to help architects establish clear relationships among strategic goals, detailed business / information management requirements, and measurable performance improvements within each area of the agency's enterprise architecture.

Financial Management consists of activities that support the interrelationships and interdependencies among budget, cost and management functions, and the information associated with business transactions.

Financial Management Systems includes systems necessary to support financial management including automated and manual processes, procedures, and 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, http://www.whitehouse.gov/omb/circulars_a127.

Funding Source means the direct appropriation or other budgetary resources an agency receives. You need to identify the budget account and the budget authority provided. Report those budget accounts providing the financing for a particular investment. Where IT investment funding is provided in a manner such that "original paying accounts" within agencies are transferring resources to a different agency account which 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 the Exhibit 53A should be that of the account which ultimately pays contracts and other costs directly, for the investment, rather than the original paying accounts. NOTE: For agencies on the IT Dashboard, funding sources are planned as the primary drivers in the algorithm to display "spending by bureau," rather than using (as in current practice) the bureau code associated with investments. This change makes it more critical that valid funding source codes be

provided in agency submissions, and will mean that a validation check on funding sources will be included in the IT Dashboard submission process for the Exhibit 53A.

Government Information means information created, collected, processed, disseminated, or disposed of by or for the Federal Government.

Information Resource Management (IRM) Strategic Plan is strategic in nature and addresses all information resources management of the agency. Agencies must develop and maintain the agency's IRM strategic plan as required by 44 U.S.C. 3506(b) (2) . IRM strategic plans should support the agency's strategic plan required in OMB Circular A–11, provide a description of how information resources management activities help accomplish agency missions delivery area and program decision, and ensure IRM decisions are integrated with management support areas including organizational planning, budget, procurement, financial management, and human resources management.

Information Security involves all functions necessary to meet federal Information Security policy requirements. It includes the development, implementation and maintenance of security policies, procedures and controls across the entire information lifecycle. This includes 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 security policy, and security audits and testing. It does not include the physical protection of facilities such as that in "Critical Infrastructure Protection" or "CIP".

Information System means a discrete set of information technology, data, and related resources, such as personnel, hardware, software, and associated information technology services organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.

Information Technology (IT) means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by an executive agency. Information Technology is related to the terms Capital Asset, IT Investment, Program, Project, Sub-project, Service, and System.

IT Investment means 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. While each asset or project would have a defined life-cycle, an investment that covers a collection of assets intended to support an ongoing business mission may not.

Major IT Investment means a program requiring special management attention because of its importance to the mission or function of the agency, a component of the agency, or another organization; has significant program or policy implications; has high executive visibility; has high development, operating, or maintenance costs; is funded through other than direct appropriations; or is defined as major by the agency's capital planning and investment control process. OMB may work with the agency to declare other investments as major investments. Agencies should consult with your OMB agency budget officer or analyst about what investments to consider as "major." Investments not considered "major" are "non-major."

Managing Partner represents the agency designated as the lead agency responsible for coordinating the implementation of the E-Gov or Line of Business (LoB) initiative. The managing partner is also responsible for coordinating and submitting the Exhibit 300 for the initiative and the Exhibit 300 will be represented as part of the managing partner's budget portfolio. Please refer to the OMB MAX portal for additional information on managing partner reporting requirements for IT investments.

New IT Investment means an IT investment and its associated projects newly proposed by the agency that has not been previously funded by OMB. This does not include investments existing within the agency that have not previously been reported to OMB.

Non-Major IT Investment means any IT investment not meeting the definition of major as defined above but is part of the agency's IT Portfolio. All non-major investments must be reported on the Exhibit 53.

On-going IT Investment means an investment and its associated assets, including both maintenance projects and operations that have 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 2012.

Operations mean the day-to-day management of an asset in the production environment and include activities to operate data centers, help desks, operational centers, telecommunication centers, and end user support services. Operational activities are reported through Section C of the Exhibit 300B. Operations costs include the expenses associated with an IT asset that is in the production environment to sustain an IT asset at the current capability and performance levels including Federal and contracted labor costs; and costs for the disposal of an asset.

Operations and Maintenance means the phase of an asset in which the asset is in operations and produces the same product or provides a repetitive service. Operations and Maintenance (O&M) is synonymous with "steady state."

Partner Agency represents the agency for an E-Gov or LoB initiative designated as an agency that should provide resources (e.g., funding, FTEs, in-kind) to the management, development, deployment, or maintenance of a common solution. The partner agency is also responsible for including the appropriate line items in its Exhibit 53 reflecting the amount of the contribution for each of the E-Gov or LoB initiatives to which it is providing resources.

Privacy Impact Assessment (PIA) is a process for examining the risks and ramifications of using information technology to collect, maintain and disseminate information in identifiable form from or about members of the public, and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting such information. Consistent with September 26th, 2003 OMB guidance (M–03–22) implementing the privacy provisions of the E-Government Act, agencies must conduct and make publicly available PIAs for all new or significantly altered information technology investments administering information in identifiable form collected from or about members of the public.

Records includes 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 and 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 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 of processed documents are not included.

Segment Architecture is a detailed, results-oriented architecture (baseline and target) and a transition strategy for a portion or segment of the enterprise. Segments are individual elements of the enterprise describing core mission areas and common or shared business services and enterprise services. They provide the core linkage of the IT Investment Portfolio to the Agency's performance management system. As such, segments are designed to be common across programs that support the same mission area. Increasingly, shared segments will be common across the government and agencies should plan to use approved government-wide shared segments as their target architecture.

Solution Architecture is a standardized method of identifying business requirements and viable technology solutions within the context of a single agency's enterprise architecture or a multi-agency sector or government-wide/international architecture. Solution architecture includes current and future views as well as transition plans at a number of levels of scope including applications, systems, segments, enterprise, sector, government-wide, national, and international. The Federal Solution Architecture Methodology (FSAM) is scheduled for release in October 2011 to provide the repeatable process for doing solution architecture.

Steady State (see "Operations and Maintenance" in this section)

Unique Investment Identifier (UII) is a persistent numeric code applied to an investment that allows the identification and tracking of an investment across multiple fiscal years of an agency's investment portfolio. The unique investment identifier is composed of a 3-digit agency code concatenated with a 9-digit unique investment number generated by the agency. Some 9-digit numbers are reserved for OMB to assign and may not be assigned by agencies, as controlled by the restrictions described below in the section on "Variable Information."

53.5 How do I determine whether I must report?

Submit an agency IT investment portfolio (Exhibits 53A) to OMB if your government agency is subject to Executive Branch review (see Section 25.1). Submit an agency security portfolio (Exhibit 53B) as required. Required agencies include all CFO Act agencies and any others as directed.

53.6 How do I submit Exhibit 53 and when is it due?

The guidance for Exhibit 53 requires agencies to submit draft and updated Exhibit 53As and final Exhibit 53Bs.

A draft Exhibit 53A shall be completed by the agency and submitted to OMB. This will allow the agency and OMB to agree to which major and non-major IT investments will be reported as part of the next President's Budget Request, and to confirm the mapping of agency investments to agency architectures. The initial draft Exhibit 53A must conform to a template described later in this section, which will be published on the OMB MAX portal, and shall be submitted to the IT Dashboard (http://www.itdashboard.gov/) by CIO Council agencies. Specific steps for completing the submission will be available on the OMB MAX portal and IT Dashboard. The completion of the initial draft Exhibit 53A should be coordinated by the agency's IT capital planning lead. At a minimum, the draft Exhibit 53A should include the legacy UPIs and current UIIs, Investment Name, and Investment Description. The draft Exhibit 53A will be due by August 31, 2011.

An updated Exhibit 53A and the Exhibit 53B are due to OMB by September 12, 2011. They must conform to a template described later in this section, which will be published on the OMB MAX portal and shall be submitted to the IT Dashboard (http://www.itdashboard.gov/) by CIO Council agencies and to the MAX Federal Community by other agencies as directed. The completion of this updated Exhibit 53A and Exhibit 53B should be coordinated and reviewed by the agency's IT capital planning office.

Additional updates to Exhibits 53A and 300A may be required after final budget decisions or if the agency requests supplemental funds that require changes to Exhibits 53A and 300A. Specific instructions and deadlines for submitting updates, corrections, and final submissions of these exhibits will be available on the OMB MAX portal and the IT Dashboard.

53.7 If I submitted Exhibit 53 last year, how do I revise it this year?

If your agency submitted Exhibits 53A&B for the FY 2012 Budget, the appropriate information can be used to create the new worksheet using the revised FY 2013 template (submissions not compliant with the provided template will be rejected). Ongoing investments must include their corresponding FY 2012 Unique Investment Identifier (UII) in the appropriate column of the Exhibit 53A. In addition, investments that were reported as major IT investments for the FY 2012 Exhibit 53A, but have a change in status for the FY 2013 Exhibit 53A must indicate so in the "Change in Investment Status Identifier" column.

It is important the exhibit is updated to reflect prior year (PY) for FY 2011, current year (CY) for FY 2012, and budget year (BY) for FY 2013. The Exhibit 53A also requires MAX funding codes for all "Funding Sources" line items. Consistent with prior submissions, "Investment Descriptions" will be limited to 255 characters.

For the purposes of Exhibit 53A only, funding sources should continue to utilize the "-9" suffix to flag funding from the American Recovery and Reinvestment Act of 2009 (ARRA).

53.8 How is the Exhibit 53 organized?

The Exhibit 53 is composed of two parts: Exhibit 53A, "Agency IT Investment Portfolio," which includes IT investment budget and architecture information, and Exhibit 53B, "Agency IT Security Portfolio," which includes a summary of agency and bureau IT security information, including IT security costs. Comparisons should be made between the two portfolios to ensure consistency.

Agency IT Investment Portfolio (Exhibit 53A)

(a) ***Overview***

Exhibit 53A is a report of all agency IT investments. Provide investment costs in millions of dollars. Reporting three decimal places (thousands of dollars) is recommended. Agencies may report up to six decimal places (whole dollars), and reporting to at least one decimal place (hundreds of thousands of dollars) is required for PY through BY.

Information reported in Exhibit 53A should be consistent with data reported in MAX schedule O, object classification (specifically, object classes 11.1 through 12.2, 23.1, 23.2, 25.2, 25.3, 25.7, 26.0, 31.0, and 41.0). All major and non-major IT investments must be reported in Exhibit 53A.

Include all Federal budgetary resources used to fund an IT investment, including discretionary or mandatory funding sources, user fees, gifts, or any other funding sources. Funding should represent only Federal budgetary resources. Do not include amounts provided by non-Federal sources, such as in matching funds for grants programs provided by State or local governments.

Funding levels in the Exhibit 53A should represent (1) budget authority for BY, reflecting the agency's budget request, (2) for CY, the best current estimate of authority available, and (3) for PY, actual amounts. These levels should be consistent with program level funding, and branch, bureau and agency summary funding tables. Funding from supplemental appropriations and the Recovery Act should also be included in a manner consistent with other budget submission displays of program data.

Exhibit 53A has six major parts:

Part 1. IT investments for Mission Delivery and Management Support.
Part 2. IT investments for Infrastructure, Office Automation, and Telecommunications.
Part 3. IT investments for Enterprise Architecture, Capital Planning and CIO Functions.
Part 4. IT investments for Grants Management Systems.

Part 5. National Security Systems IT Investments.
Part 6. Grants to State and Local IT Investments.

All parts use the following common data elements:

- ***Agency Description of Change in Investment Status*** is used when an indicator has been chosen for "Change in Investment Status" to provide more description of the rationale for the change which may include impacted UPIs, specific reference to legislative requirements, or governance board decisions and effective dates.

- ***Agency Funding*** is the agency's budgetary resources for a given investment.

- ***Change in Investment Status*** is used when an investment has a change in status (i.e. downgraded to non-major, eliminated, retired, consolidated, split) for the current budget submission relative to the previous budget cycle. The change of status should be indicated with one of the following reasons: 1) (Downgraded)Downgraded to non-major because it does not fit the criteria for Major investment, or because of insufficient activities or funding, 2)(Split) This consolidated investment is no longer included in Major Investments, due to the split up into separate component investments 3)(Consolidated) this investment is no longer a major investment, due to consolidation of activities into another investment 4)(Re-aligned) Investment was subject to agency-wide realignment of the IT portfolio, 5)(Retired) Investment was retired, 6)(Eliminated) Investment was eliminated or 7)(Upgraded) Upgraded to Major Investment, 8) Other, 0)None.

- ***Cross-Boundary Information Sharing*** is one that crosses a bureau or agency boundary, including information sharing with international, State, local, tribal, industry, or non-governmental organization partners. If the investment supports reusable, standardized information exchanges indicate which: 1) NIEM, 2) UCORE, 3) XBLR, 4) Other 0) None.

- ***Current UII*** includes two parts: an agency code and a 9-digit unique identifier. Variable information formerly included in the UPI in previous years is not part of the UII primary key. Details are provided in Section 53.9.

- ***Development/Modernization/Enhancement Expenditures*** (corresponding to capitalized costs) are the costs for projects leading to new IT assets and projects that change or modify existing IT assets to: improve capability or performance; implement legislative or regulatory requirements; or to meet agency leadership requests. These expenses include: hardware; software; Federal and contracted labor for planning, development, acquisition, system integration; and direct overhead and project management. If the replacement of non-repairable or non-working IT hardware or software to continue the operation of an asset improves the capability or performance of an asset, the expense should be categorized as operations.

- ***FEA mapping codes captured in the Ex 53a are as follows:*** The first 3-digit code indicates the business area served by this investment (the 3-digit BRM sub-function code). The second 3-digit code indicates the services also associated with this investment (the service component code). Guidance on the codes for these mappings can be found at http://www.whitehouse.gov/omb/e-gov/fea/.

- ***Funding Source*** See definition in section 53.4. For each funding source, identify the budgetary resources including the MAX funding codes used for the investment. This is required for all investments. Add as many funding source line items as are appropriate for the investment. To avoid double counting or under counting, the totals of the funding amounts for a investment must match the main investment line item, represented with the investment category of "00" or "24" or "48."

- ***Homeland Security Priority Identifier*** means an IT investment supporting the homeland security mission areas of 1) Intelligence and warning, 2) Border and transportation security, 3) Defending against catastrophic threats, 4) Protecting critical infrastructure and key assets, 5) Emergency preparedness and response, 6) Other, 0) None. If the investment supports one of these mission areas, indicate which one(s) by listing the corresponding number(s) listed above.

- ***Investment Description*** means a short public description (limited to 255 characters) for each investment (major, migration, partner contribution, and non-major). This description should explain the purpose of the investment and what program(s) it supports, including the value to the public. This description should be understandable to someone who is not an expert of the agency. If the investment is part of a multi-agency initiative or part of another business case, please provide description of where that business case is located in the appropriate agency Budget submission (i.e. managing partner UII). For example, if the investment represents your agency's participation in one of the Presidential initiatives, the description should state that this investment represents your agency's participation in one of the Presidential initiatives and should refer to the UII of the managing partner's business case (i.e. managing partner UII).

- ***Investment Title*** means a definitive title explaining the investment. If the investment title has changed, include the previous name in parentheses. For "funding source" information, provide the 10- digit OMB MAX account code (OMB Circular A-11, Section 79.2). Additional information can be found in Part III of this circular. For the purposes of Exhibit 53 only, funding sources should continue to utilize the "-9" suffix to flag funding from the American Recovery and Reinvestment Act of 2009 (ARRA).

- ***Operations & Maintenance (O&M, or Steady-State costs)*** describes the expenses associated with an IT asset that is in the operations and maintenance life cycle phase. Operations expenses including maintenance projects and operation costs needed to sustain the IT asset at the current capability and performance levels including: Federal and contracted labor costs; corrective hardware and software maintenance; voice and data communications maintenance and service; replacement of broken or obsolete IT equipment; and overhead costs.

- ***Previous Unique Project Identifier (UPI)*** means the identifier depicting agency code, bureau code, part of the Exhibit 53 where investment will be reported, mission area, type of investment, agency four-digit identifier, and two-digit investment category code used to report the investment in any previous Exhibit 53 submission to OMB. Indicating the UPI used for a previous submission allows cross-walk and historical analysis crossing fiscal years for tracking purposes. Previous UPI is mandatory, with the exception of new investments. More than one entry is possible to indicate consolidation of previous UPIs (comma separated).

- ***Solution Architecture*** is a standardized method of identifying business requirements and viable technology solutions within the context of a single agency's enterprise architecture, or a multi-agency sector or government-wide/international architecture. Solution architecture includes current and future views as well as transition plans at a number of levels of scope that include applications, systems, segments, enterprise, sector, government-wide, national, and international. The Federal Solution Architecture Methodology (FSAM) is scheduled for release in October 2011 to provide the repeatable process for doing solution architecture.

- ***Steady State costs***, see Operations & Maintenance in this section

- ***Supports Information Sharing, Access and Protection*** means an IT investment supporting the information sharing, access, and protection mission areas of: 1) the National Network of State and Major Urban Area Fusion Centers; 2) Assured Interoperability across Controlled Unclassified Information (CUI)/Sensitive but Unclassified (SBU) networks targeting federal, state, local, and tribal law enforcement, public safety, homeland security, and intelligence personnel; 3) Assured Interoperability

across Classified SECRET networks; 4) Nationwide Suspicious Activity Reporting Initiative; 5) Cargo Screening; and 6) Data Aggregation, or 0) none. If the investment supports one of these mission areas, indicate which one(s) by listing the corresponding number(s) listed above

(b) ***Part 1. IT investments for Mission Delivery Areas and Management Support Areas***[1]

Consistent with your agency's strategic and annual performance plan, report amounts for IT investments directly supporting an agency-designated mission delivery area or management support area (e.g., mission delivery area means programs or activities that execute the agency mission as outlined in the agency strategic plan. Management support area means activities such as human resource management, financial management, command and control). Report each area in which IT investments are funded, itemizing the "major" and "non-major" IT investments within each mission area. Include capital costs (planning, development, modernization, and enhancement) and operation and maintenance expenses for each IT investment in this part of Exhibit 53.

Agencies must have an area titled "Financial Management", and it must be reported as the first area. Report all IT investments for major financial management systems in this area.

(c) ***Part 2. IT investments for Infrastructure, IT Security, Office Automation, and Telecommunications***

Report all IT investments supporting planning, development, modernization, enhancement, operation, and maintenance of common user systems such as IT infrastructure and IT security. Each agency may have multiple Exhibit 300s encompassing office automation, infrastructure, security, and telecommunications for the agency. These investments may be defined at the bureau level, and/or by functional components of infrastructure. These IT infrastructure investments may support multiple mission areas and should include End User Services and Support, Mainframes and Servers Services and Support, and Telecommunications Services and Support. IT infrastructure includes direct costs (that produce tangible IT products or services for business users) and indirect costs (that do not lead to a tangible product or direct support of business users), such as IT program management costs and overhead expenses.

Agencies are encouraged to report these investments as they are managed. If IT infrastructure is managed at both the agency and bureau levels, then report both agency and bureau-level infrastructure investments.

Report IT security investments (including agency- and bureau-level IT security programs) on a separate line.

(d) ***Part 3. IT investments for Enterprise Architecture, Capital Planning and CIO Functions***

Report amounts for IT investments supporting strategic management of IT operations (e.g., business process redesign efforts not part of an individual investment, enterprise architecture development, capital planning and investment control processes, procurement management, and IT policy development and implementation). IT investments in this part of Exhibit 53A should include costs for Chief Information Officer (CIO) functions.

(e) ***Part 4. IT investments for Grants Management Systems***

Report on IT investments information in this part of Exhibit 53A that support the planning, development, modernization, enhancement and operation of grants management systems.

(f) ***Part 5. National Security Systems investments***

[1] For the purpose of Ex 53, IT Investments for Enterprise Architecture, Capital Planning and CIO functions remain in Part 3. IT Investments for Grants Management Systems remain in Part 4.

Report on IT investments this part of Exhibit 53A that representing planning, development, modernization, enhancement and operation of National Security Systems. Only DoD may use this part.

(g) ***Part 6. Grants to State and Local IT investments***
Report amounts for grants to State and Local that fund the planning, development, modernization, enhancement and operation of State and Local IT systems. Agencies should only use this part to report "Grants to State and Local." Before using Part 6 for anything other than these types of investments, please check with your agency's OMB E-Gov analyst.

Agency Security Portfolio (Exhibit 53B)

The Agency Security Portfolio is to be completed at the agency level, not at the individual investment level. Exhibit 53B uses the following data elements (in order as they appear in the Exhibit 53B). Note that eight data elements formerly provided separately, still described below, are to be reported in the aggregate of "Total IT Security Tools Costs."

- ***Total IT Security Tools Costs (Anti-Virus)***—a program that monitors desktops/laptops to identify all major types of viruses and prevents or contain virus incidents.
- ***Total IT Security Tools Costs (Anti-Malware)***—a program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.
- ***Total IT Security Tools Costs (Data leakage protection tools***)—systems designed to detect and prevent the unauthorized use and transmission of confidential information including encryption for PII.
- ***Total IT Security Tools Costs (Email Filtering Software***)—software that organizes e-mail according to defined criteria, most commonly used for detecting and eliminating spam and malware.
- ***Total Security Tools Costs (Intrusion Detection System - IDS)***—software that looks for suspicious activity on networks and alerts administrators.
- ***Total IT Security Tools Costs (Intrusion Prevention System - IPS)***—systems which can detect an intrusive activity on networks and can also attempt to stop the activity, ideally before it reaches its targets.
- ***Total IT Security Tools Costs (Security Information Management/Security Information and Event Management - SIM/SIEM)—***software/systems that collect security data (e.g. event logs) into a central repository for trend analysis.
- ***Total IT Security Tools Costs (Web filtering software— also known as Content-Control software or Censorware)*** software designed and optimized for controlling what content is permitted to a reader, especially when it is used to restrict material delivered over the Web. Content-control software determines what content will be available.

53.9 How is Exhibit 53A coded?

Use the following UII 12-digit line number coding, and additional six 2-digit Variable Information fields, to categorize investments and line structure for your Exhibit 53A (Each investment identified in the agency's portfolio must have a unique UII):

Entry	Description
	Unique Investment Identifier Primary Key
XXX–xxxxxxxxx	The first three digits are your agency code (see Appendix C of OMB Circular A-11).

xxx–**XXXXXXXXX**	Unique Identifier: a nine digit number which may be separated into segments for agency used but which must be reported as a continuous string of digits (xxxxxxxxx). This identifier should be system generated, applied at the agency level, and will allow agencies up to one billion unique identifiers to associate with IT investments. Once used, the unique identifier must be retired. That is, if an IT investment is retired, discontinued, or merged with another IT investment, the unique identifier persists with that IT investment. (Note: 99999XXXX – codes are reserved for Approved Multi-Agency investments, including E-Gov and LOB initiatives)
Variable Information: The following attributes extracted from the old UPI will continue to be supplied.	
XX-xx-xx-xx-xx-xx	00 = Code for all investments other than those coded "24" or "48." 24 = E-Gov initiatives or an individual agency's participation in one of the E-Gov initiatives 48 = Other than E-Gov initiatives, any multi-agency collaboration or an individual agency's participation in one of the multi-agency initiatives.
xx-**XX**-xx–xx-xx-xx	The next two digits are your bureau code (see Appendix C of OMB Circular A-11). If this is a department only or an agency-wide activity, use 00 as your bureau code.
xx-xx-**XX**-xx-xx-xx	These two digits indicate the six parts of the Exhibit 53: 01 = Part 1. IT investments for Mission Delivery and Management Support Area 02 = Part 2. IT investments for Infrastructure, IT Security, Office Automation, and Telecommunications 03 = Part 3. IT Investments for Enterprise Architecture, Capital Planning, and CIO Functions 04 = Part 4. IT Investments for Grants Management Systems 05 = Part 5. National Security Systems (DoD Only). 06 = Part 6. Grants to State and Locals
xx-xx-xx-**XX**-xx-xx	These two digits indicate the mission delivery and management support area. Assign a unique code for each mission delivery and management support area reported.
xx-xx-xx-xx-**XX**-xx	These two digits indicate your agency's type of investment. Select one of the following two digit codes according to the type of investment you are reporting: 01 = Major IT investments (see definition in Section 53.4) 02 = Non-major IT investments (see definition in Section 53.4) 03 = IT migration investment 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 UPI of the major asset investment of the managing partner. 04 = Partner agency funding contribution represents resources provided by partner agency for a joint effort for more than one agency. Use the 04 indicator to identify investments

	where the business case for the major IT investment is reported in another agency's Exhibit 53. Description of the IT investment should indicate the UPI of the major asset investment of the managing partner.
xx-xx-xx-xx-xx-**XX**	These two digits identify the nature of the "line item" in the Exhibit 53 structure for both the XML format used for agencies on the IT Dashboard, and the line number in an equivalent spreadsheet file (CSV or XLS file), for agencies not on the IT Dashboard: 00 = Total investment title line, structurally the first line for reporting this particular investment. 04 = Funding source or appropriation. [09 = Any subtotal – This value is used only for agencies not on the IT Dashboard].

Use the following 10 digit number coding system to update or complete your OMB MAX Account ID code information:

Entry	Description
XXX–xx–xxxx–x	The first three digits are your agency code (see Appendix C of OMB Circular A-11).
xxx–**XX**–xxxx–x	The next two digits are your bureau code (see Appendix C of OMB Circular A-11).
xxx–xx–**XXXX**-x	This is a four-digit Account Symbol for the appropriate MAX Account. (see Section 79.2 of OMB Circular A-11)
xxx–xx–xxxx-**X**	This is a single digit Transmittal Code. (see Section 79.2 of OMB Circular A-11)

Use the following 6 digit number coding system to identify each investments segment architecture ID (for additional guidance, please refer to EASR Interim v1.3):

Entry	Description
XXX-xxx	The first three digits identify the investment's agency segment (registered with the FEA PMO)
xxx-**XXX**	The final three digits identify the investment's federal standard segment. Select one of the following three digit codes to map investments to federal standard segments: **Entry---Description** 000—No Standard Segment 100—IT Infrastructure 150—IT Management 170—Information Security 200—Information Sharing 220—Information Management and Dissemination 300—Identity Credential and Access Management 310—Geospatial Services

400—Health: Access to Care
402—Health: Consumer Empowerment
404—Health: Health Care Administration

406—Health: Health Care Delivery Services
408—Health: Health Care Research and Practitioner Education
410—Health: Population Health Management and Consumer Safety
500—Financial Management
510—Budget Formulation
550—Human Resources Management
600—Acquisition Management
620—Facilities Management
640—Supply Chain Management

53.10 What are the steps to complete Exhibit 53?

Exhibit 53 is separated into two main exhibits. Exhibit 53A provides information on the agency's IT investment portfolio, while Exhibit 53B provides information on the agency's IT security portfolio. The following provides step-by-step instructions to complete each part of Exhibit 53A and 53B. See Exhibit 53.4 and 53.8 for definitions.

AGENCY IT INVESTMENT PORTFOLIO

Entry	Description
Part 1. IT investments for Mission Delivery Area and Management Support Area	Report IT investments that directly support an agency-designated mission delivery and management support area. Report each mission delivery and management support area in which IT investments are funded. This information should map directly to your agency's strategic and annual performance plan. For IT investments that cover more than one agency, report in the mission area with oversight of the IT investment. Mission delivery and management support area 01 is reserved for IT investments for major financial management systems. **Step 1:** For each mission delivery and management support area, list each major IT investment and the corresponding investment costs. If this IT investment supports Homeland Security (HS) goals and objectives (see Section 53.8a) provide the number for the HS mission area. **Step 2:** For each mission delivery and management support area, list each non-major investment. If a system or investment supports Homeland Security goals and objectives (see Section 53.8.a), answer yes.

Part 2. IT investments for Infrastructure, IT Security, Office Automation, and Telecommunications	IT investments for Infrastructure, IT Security, Office Automation, and Telecommunications are reported in Part 2 of Exhibit 53A. Report all IT investments supporting common user systems, security, communications, and computing infrastructure. Each agency may have multiple Exhibit 300s encompassing office automation, infrastructure, IT Security, and telecommunications for the agency. It is encouraged that these investments be reported at the point of management and thus may be defined at the bureau level, and/or by functional components of infrastructure. These may involve multiple mission areas and include End User Systems and Support, Mainframes and Servers Services and Support, and Telecommunications Services and Support. All IT Investments capturing these shared services are to be included in Part 2.
Part 3. IT Investments for Enterprise Architecture, Capital Planning and CIO Functions	Each agency should list all enterprise architecture, IT capital planning, and CIO function investments. For the President's Budget, enterprise architecture, IT capital planning, and CIO function investments are not categorized as major investments and an Exhibit 300 is not required for them. Any capital planning and investment control process investments may be reported separately in this section. However, agencies should ensure that investments identified in Variable information coding as belonging in Part 3 of the Exhibit 53A have the correct primary FEA mapping in order to clearly distinguish the EA investments from other planning investments (e.g., EA investments should be mapped to the "Enterprise Architecture" sub-function in the BRM).
Part 4. IT Investments for Grants Management Systems	Report IT investments that support grants management operations. See classification instructions in Section 53.8.a under Grants Management.
Part 5. National Security Systems	Report IT investments related to National Security Systems (Defense Only).
Part 6. Grants to State and Local	Report BRM coding (3-digit Sub-function code only), total amounts for PY, CY and BY (DME & SS) for IT investments for Grants to State and Local. All other fields are optional.

AGENCY IT INVESTMENT PORTFOLIO (COLUMNS)

These columns are required for the President's Budget Exhibit 53A, Agency IT Investment Portfolio:

Column 1: Previous UPI (17–digits required for all legacy investments)

Column 2: Current UII (12–digits primary key)

Column 3: Investment Category (2 digit code)

Column 4: Bureau Code (2 digit code) (variable element)

Column 5: Part of Exhibit 53 (2 digit code) (variable element)

Column 6: Mission Delivery and Management Support Area (2 digit code) (variable element)

Column 7: Type of Investment (2 digit code) (variable element)

Column 8: Line Item Descriptor (2 digit code) (variable element)

Column 9: Change in Investment Status Identifier (1 digit code)

Column 10: Agency description of change in investment status (limited to 255 characters)

Column 11: Investment Title

Column 12: Investment Description (limited to 255 characters)

Column 13: FEA BRM Mapping - Sub-Function (3 digit code)

Column 14: Service Code Mapping - Component (3 digit code)

Column 15: Segment Architecture – Agency Segment (3 digit code)

Column 16: Segment Architecture - Federal Standard Segment (3 digit code)

Column 17: Homeland Security Priority Identifier (select all that apply)

Column 18: Cross-Boundary Information Identifier (1 digit code)

Column 19: Supports Information Sharing, Access and Protection (select all that apply)

Column 20: DME [Planning, Development/Capital Spending] (PY/2011) Agency Funding ($M)

Column 21: DME [Planning, Development/Capital Spending] (PY/2011) Contributions ($M)

Column 22: DME [Planning, Development/Capital Spending] (CY/2012) Agency Funding ($M)

Column 23: DME [Planning, Development/Capital Spending] (CY/2012) Contributions ($M)

Column 24: DME [Planning, Development/Capital Spending] (BY/2013) Agency Funding ($M)

Column 25: DME [Planning, Development/Capital Spending] (BY/2013) Contributions ($M)

Column 26: Operational & Maintenance Spending [non-DME] (PY/2011) Agency Funding ($M)

Column 27: Operational & Maintenance Spending [non-DME] (PY/2011) Contributions ($M)

Column 28: Operational & Maintenance Spending [non-DME] (CY/2012) Agency Funding ($M)

Column 29: Operational & Maintenance Spending [non-DME] (CY/2012) Contributions ($M)

Column 30: Operational & Maintenance Spending [non-DME] (BY/2013) Agency Funding ($M)

Column 31: Operational & Maintenance Spending [non-DME] (BY/2013) Contributions ($M)

AGENCY IT SECURITY PORTFOLIO (Exhibit 53B)

	Row	Description
1	Agency Code	Three digit agency identifier (see Appendix C of OMB Circular A-11)
2	Number of Government FTEs with information security responsibilities	Report number of Government employees with information security responsibilities, including the fractional portion of those who devote a percentage of their time to these responsibilities. This count should include but not be limited to: Designated Security Officers, Network security staffs, System Administrators, and system owners and should not include individuals responsible for physical security such as guards. The number should be rounded to two decimal places.
3	Average cost per Government FTE with information security responsibilities	Using the salary information of the Government employees counted in "Number of Government FTE with Security Responsibilities", calculate an average fully loaded cost per Government FTE. The average cost should be represented in dollars and rounded to two decimal places.
4	Number of contractor FTEs with information security responsibilities	Report the number of contractor staff with information security responsibilities including the fractional portion of those who devote a percentage of their time to these responsibilities. The number should be rounded to two decimal places.
5	Average cost per contractor FTE for information security responsibilities	Using the billing rate of the contract staff counted in "Number of contractor FTEs with information security responsibilities" calculate an average yearly cost per contractor FTE. The average cost should be represented in dollars rounded to two decimal places.
6	Total IT Security Tools Cost	(This is the sum of the eight data elements formerly provided separately in the Ex. 53B for the FY 2012 Budget cycle). Costs should be reported in thousands and reported to the dollar. 1. **Anti-Virus Software Licensing Costs** - The licensing costs incurred or expected to be incurred for the respective budget year. If an agency does not purchase anti-virus software separately from anti-malware software, please enter all costs on the line for anti-malware and leave this line blank. 2. **Anti-Malware Software Licensing Costs** - The licensing costs incurred or expected to be incurred for the respective budget year. 3. **Intrusion Detection Systems Licensing Costs** - The licensing costs incurred or expected to be incurred for the respective budget year. If you have an IDS which is part of an Intrusion Prevention System (IPS), please include all costs in IPS and do not list here. Please include the amount paid for the Managed Trusted Internet Protocol Service via the Networx contract, as well as any other operational IDS. 4. **Intrusion Prevention Systems Licensing Costs** - The licensing costs incurred or expected to be incurred for the respective budget year. 5. **Web Filtering Software Licensing Costs** - The licensing costs incurred or expected to be incurred for the respective budget year. Costs should be reported in thousands and reported to the dollar.

		6. **Email Filtering Software** - The licensing costs incurred or expected to be incurred for the respective budget year. If an agency does not purchase email filtering software separate from web filtering software, please include all costs in web filtering software and do not list here. 7. **SIM/SIEM tools** - Report the tool costs incurred or expected to be incurred for the respective budget year. 8. **Data Leakage Protection tools** - Report the tool costs incurred or expected to be incurred for the respective budget year.
7	Costs for NIST 800-37 implementation	Report the costs incurred or expected to be incurred for the respective budget year. Costs should be reported in thousands and reported to the dollar. Security Authorization costs should only include contract costs.
8	Number of systems scheduled for activities represented in Row 7.	Number of systems used to in cost calculations for "Costs for NIST 800-37"
9	Costs for annual FISMA testing	Report the costs incurred or expected to be incurred for the respective budget year. Costs should be reported in thousands and reported to the dollar. Please include all costs including licensing of tools, services and FTEs.
10	Costs for network penetration testing activities	Report the costs incurred or expected to be incurred for the respective budget year. Costs should be reported in thousands and reported to the dollar. Please include all costs including licensing of tools, services and FTEs
11	Security awareness training costs	Report the costs incurred or expected to be incurred for the respective budget year. Costs should be reported in thousands and reported to the dollar. This should include the costs of annual security awareness training required by the FISMA Act.
12	Security training costs for employees with significant security responsibilities	Report the costs incurred or expected to be incurred for the respective budget year. Costs should be reported in thousands and reported to the dollar. This does not include the annual awareness training.

Note the Exhibit 53B should not include security costs typically embedded in investments such as destruction of data (e.g. degaussing, shredding, etc), physical or logical access control or physical access control software, continuous monitoring software, tracking and reporting software, and annual disaster recovery and contingency plan tests.

AGENCY IT SECURITY PORTFOLIO (ROWS)

These rows are required for the President's Budget Exhibit 53B, Agency IT Security Portfolio, and should be reported for the PY, CY and BY respectively:

Row 1: Agency ID

Row 2: Number of government FTEs with information security responsibilities

Row 3: Average cost per Government FTE with information security responsibilities

Row 4: Number of contractor FTEs with information security responsibilities

Row 5: Average cost per contractor FTE for information security responsibilities

Row 6: Total IT Security Tools Costs

Row 7: Costs for implementation and activities associated with NIST 800-37 of systems

Row 8: Number of systems scheduled for the activities represented in Row 7.

Row 9: Annual FISMA testing costs

Row 10: Network penetration testing activities costs

Row 11: Security awareness training costs

Row 12: Security training costs for employees with significant security responsibilities