SECTION 53—INFORMATION TECHNOLOGY AND E-GOVERNMENT

Table of Contents

Summary of Changes

Significantly updates exhibit 53 requirements. In particular:

Updates special terms related to IT and E-Government (section 53.4).

Requires agencies to submit an initial draft of exhibit 53 to OMB by August 27, 2010 and a final on September 13, 2010; draft and final exhibits must be submitted electronically via Federal IT Dashboard (section 53.6).

Requires agencies to provide a breakout of infrastructure costs by MSSS, TSS, and EUSS for the budget year (section 53.10).

Requires agencies to report on cross-boundary information sharing and Data.gov integration (section 53.10).

Requires agencies to report security budget data using Exhibit 53B (section 53.10).

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

The information required allows the agency and 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:

- Ensure initiatives create a citizen-centered electronic presence and advance an E-Government (E-Gov) strategy including specific outcomes to be achieved;
- Understand the amount being spent on development and modernization of IT versus the amount being spent on operating and maintaining the status quo for IT;
- Identify costs for providing IT security as part of agency investment life cycle as well as IT security costs for supporting crosscutting or infrastructure related investments under the Federal Information Security Management Act (FISMA);

- Provide a full and accurate accounting of IT investments for the agency as required by the Clinger-Cohen Act of 1996;

- Ensure spending on IT supports agency compliance with the requirements of Section 508 of the Rehabilitation Act Amendments of 1998 (Electronic and Information Technology Accessibility) and Section 504 of the Rehabilitation Act of 1973 (Reasonable Accommodation);

- Ensure compliance with E-Government Act of 2002 and Paperwork Reduction Act of 1995;

- Ensure privacy is considered and protected in electronic activities;

- Identify investments supporting Homeland Security goals and objectives; and

- Review requests for agency financial management systems.

Agencies must provide this information using the Agency IT Investment Portfolio (exhibit 53) reporting format. This information should be consistent with information required in section 51.3. In addition, as an output of your agency's internal 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 Part 7 (section 300) of this Circular.

The total investment's costs must cover the entire risk-adjusted life cycle of each system and include all budgetary resources (direct appropriation, working capital fund, revolving funds, etc.). Budgetary resources are defined in section 20 of this Circular. Life cycle costs should also be risk adjusted to include any risks addressed on the Capital Asset Plan and Business Case. These total investment costs must be formulated and reported in order for OMB to meet the Clinger-Cohen Act's requirement which states, 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 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 this Circular (see section 220).

- 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 section 52 of this Circular.

- 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 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 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), 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.

- 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 IT investments improve program performance?

All IT investments must clearly demonstrate 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 documenting in a Segment of the Agency's Enterprise Architecture. The capital asset plans and business cases (exhibit 300) and "Agency IT Investment Portfolio" (exhibit 53) demonstrate the agency management of IT investments and how these governance processes are used when planning and implementing IT investments within the agency. Any attendant documentation should be maintained and readily available if requested by OMB.

The individual agency's exhibit 53 is used to create an overall "Federal IT Investment Portfolio" published as part of the President's Budget. OMB's portfolio review and Budget process will ensure IT investments support the strategy identified in this section and ensure the Federal IT Investment Portfolio includes the most effective portfolio of investments to:

- Improve the management of programs to achieve better program outcomes;
- Eliminate redundant or non productive IT investments through multi-agency collaboration;
- Support the Federal Enterprise Architecture (FEA) and the Agency Enterprise Architecture;
- Support Presidential initiatives and E-Gov strategy;
- Focus IT spending on high priority modernization initiatives;
- Manage major IT investments within 10% of cost, schedule, and performance objectives

53.4 What special terms should I know?

Budget Execution represents activities associated with the legal and managerial uses of budgetary resources to achieve results that comply with the enacted Budget and Administration policy. Budget execution activities include but are not limited to: apportionments, allotments, commitments, reprogramming actions, incurring obligations, and funds control. See sections 120 through 150 of Part 4 of OMB Circular No. A-11 for a comprehensive list of Budget execution activities.

Budget Formulation represents activities undertaken to determine priorities for future spending and to develop an itemized forecast of future funding and expenditures during a targeted period of time. This includes the collection and use of performance information to assess the effectiveness of programs and develop Budget priorities.

Business Reference Model (BRM) one of five reference models of the Federal Enterprise Architecture**,** is a function-driven framework used to describe the lines of business and sub-functions performed by the Federal Government independent of the agencies performing them. IT investments are mapped to the BRM to identify collaboration opportunities.

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.

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. This cloud model promotes availability and is composed of five essential characteristics (on-demand self service, broad network access, resource pooling, rapid elasticity, and measured service), three service models (software as a service, platform as a service, and infrastructure as a service), and four deployment

models (private, community, public and hybrid). Please note that cloud computing is an evolving paradigm, and its definition will continue to evolve. See NIST definition of Cloud Computing

Core Financial System is an information system that may perform all financial functions including general ledger management, funds management, payment management, receivable management, and cost management. The core financial system is the system of record that maintains all transactions resulting from financial events. It may be integrated through a common database or interfaced electronically to meet defined data and processing requirements. The core financial system is specifically used for collecting, processing, maintaining, transmitting, and reporting data regarding financial events. Other uses include supporting financial planning, budgeting activities, and preparing financial statements. Any data transfers to the core financial system must be: traceable to the transaction source; posted to the core financial system in accordance with applicable guidance from the Federal Accounting Standards Advisory Board (FASAB); and in the data format of the core financial system.

Federal Enterprise Architecture (FEA) is a business-based framework for government-wide improvement. It describes the relationship between business functions and the technologies and information supporting them. The FEA is constructed through a collection of interrelated "Segment Architectures" and "reference models" designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across federal agencies. For the next President's Budget, major IT investments should be aligned with each reference model within the FEA framework. More information about the FEA reference models is available at http://www.whitehouse.gov/omb/e-gov/fea.

Federal Segment Architecture Methodology (FSAM) – is a scalable and repeatable step-by-step process for developing and using segment architectures developed by distilling proven best practices from across Federal agencies. Use of the FSAM should result in more complete and consistent segment architecture products by helping architects engage segment leaders 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 the segment.

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

Financial Management System includes the core financial systems and the financial portions of mixed 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.

Financial Operations represent activities associated with processing, recording, and reporting of revenues, receipts, disbursements, expenditures, assets, liabilities, and other financial transactions; reconciliation of asset and liability accounts, such as accounts or loans receivable, with subsidiary records and with external data, such as Treasury cash records; and preparing financial statements.

Financial System (See financial management system, core financial system, and mixed financial system.)

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.

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

Green IT refers to the application of sustainable and environmentally efficient practices so that computing resources are used in a sustainable and environmentally efficient manner. Green IT applies to a broad range of activities that span the entire IT capital asset lifecycle, including but not limited to (a) research and development; (b) manufacturing; (c) acquisition; (d) operations/use; and (e) disposition. Sustainable computing practices should be integrated into agency capital planning processes.

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, and ensure IRM decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions.

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, as defined by the Clinger-Cohen Act of 1996, sections 5002, 5141, and 5142, means any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For purposes of this definition, equipment is "used" by an agency whether the agency uses the equipment directly or it is used by a contractor under a contract with the agency that (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

Information Technology Migration Investment means the partner agency's migration costs associated with moving an existing investment, system, process or capability to a Government-wide common solution. All IT E-Gov and Line of Business (LoB) migration projects may be tracked separately and not part of a larger investment.

Infrastructure as a Service (IaaS) is 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 application. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g. host firewalls).

Major IT Investment means a system or an acquisition requiring special management attention because it: has significant importance to the mission or function of the agency, a component of the agency or another organization; is for financial management and obligates more than $500,000 annually; 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. If you are unsure about what investments to consider as "major", consult your agency budget officer or OMB representative. 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 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.

Mixed Financial System is an information system that can support both financial and non-financial functions.

New IT Project means an IT investment 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 initiative or investment not meeting the definition of major defined above but is part of the agency's IT Portfolio. All non-major investments must be reported individually on the exhibit 53.

On-going IT Investment means an investment that has been through a complete Budget cycle with OMB and represents Budget decisions consistent with the President's Budget for the current year (BY–1).

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.

Partner Agency IT "fee-for-service" represents the financial fees paid for by a partner agency for IT services provided.

Platform as a Service (PaaS) is the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages 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 application hosting environment configurations.

Primary FEA Mapping is the identification of the primary function this IT investment supports. For the next President's Budget, investments should identify a primary mapping to the BRM (Line of Business and associated sub-function). Only one primary FEA mapping should be provided for each investment. A BRM mapping should be used if the investment primarily supports a functional area. Guidance on the BRM codes for the primary mappings can be found at http://www.egov.gov. Note: BRM lines of business and sub-functions in the Mode of Delivery business area are not valid as primary FEA mappings.

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 and provides 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 government and agencies should plan to use approved government-wide shared segments as their target architecture.

Software as a Service (SaaS) is the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). 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.

Validated E-Gov Standard means a private, voluntary or U.S. government-developed standard developed and adopted via a widely recognized and broadly accepted process. These standards have been validated for use by NIST. The E-Gov standard validation process and validated standards can be located at the NIST E-Gov Standards Resource Center.

53.5 How do I determine whether I must report?

Submit an agency IT investment portfolio (exhibit 53) to OMB if your government agency is subject to Executive Branch review (see Section 25.1).

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

Section 53 requires the submission of both a draft exhibit 53A, and a budget request exhibit 53A and exhibit 53B.

An initial draft of the exhibit 53A should be submitted in order for OMB and the agency to agree on what major investments and non-major investments will be reported for the next President's Budget process, and establish the mapping of agency investments to agency architectures. The draft exhibit 53A should conform to a template described later in this section, to be made available electronically to the IT Dashboard (http://it.usaspending.gov/) in time for agency submission. Specific steps for completing the submission will be available on the IT Dashboard. Draft exhibit 53A submissions should be coordinated providing input from both IT capital planning leads, and the agency's chief architect, to conform with guidance on segment architecture. At a minimum, the Draft exhibit 53A should include the legacy and current UPIs, Investment Name and Investment Description. Draft 53As will be due by August 27, 2010.

You must submit the draft exhibit 53A in an electronic format, via XML feed, to the Federal IT Dashboard.

Your budget request, exhibit 53A and exhibit 53B, is due to OMB by September 13, 2010, and should conform to the templates described later in this section. The budget request and any subsequent updates pr corrections must be submitted via the IT Dashboard. Updates should include a coordinated update after final budget decisions, of the exhibits 53A and 53B and the accompanying Capital Asset Plans and Business Cases (exhibit 300), reflecting all final budget decisions. Specific instructions for submitting updates and corrections of the exhibit will be available on the IT Dashboard.

If agencies are requesting supplemental funds, which include changes to the agency's portfolio, as part of their supplemental request, agencies should submit an updated exhibit 53.

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

If your agency submitted an exhibit 53 for the 2010 Budget, the appropriate information can be used to create the new worksheet using the provided FY 2012 template (submissions not compliant with the provided template will be rejected). Ongoing investments from FY 2011 to FY 2012, must include their corresponding FY 2011 Unique Project Identifier(s) (UPI) in the appropriate column of the Exhibit 53. In addition, investments that were Major investments in 2011, but have a change in status in 2012 must indicate so in the "Change in Investment Status Identifier" column. It is important the file is updated to reflect PY for FY 2010, CY for FY 2011, and BY for FY 2012. The Exhibit 53 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 53 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 exhibit 53 organized?

The exhibit 53 is composed of two parts: 53A Agency IT Investment Portfolio which includes investment level budget information and 53B Agency Security Portfolio which includes portfolio level security budget information. Comparisons should be made between the two portfolios to ensure consistency.

Agency IT Investment Portfolio (Exhibit 53A)

(a) ***Overview***

As a general rule, exhibit 53A covers IT investments for your agency as a whole. Provide investment amounts in millions of dollars (agencies may provide up to six decimal points, at least one decimal point is required) for PY through BY. It is recommended that no more than three decimal points be provided. Information reported here should be consistent with data you report 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). Include all major IT investments, including financial management systems, reported in exhibit 300 as well as all migration, partner agency funding contribution, and non-major IT investments.

IT investments and funding levels should be provided whether funding is from discretionary or mandatory funding sources, and should include investments funded by user fees, gifts, or any other funding sources. Funding levels should represent Federal funding, and should not include amounts provided by non-Federal sources, such as in grants programs with State or Local matching.

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 including unobligated amounts, and (3) for PY, actual amounts. These levels should be consistent at the agency and bureau level with how program level funding, and bureau or agency summary funding tables, in how overall funding levels are treated. Inclusion of 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 Area Support.
- Part 2. IT investments for Infrastructure, Office Automation, and Telecommunications.
- Part 3. IT investments for Enterprise Architecture and Planning.
- 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:

- ***Previous Unique Project Identifier (UPI)*** means the unique project identifier 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).

- ***Current UPI*** means the identifier depicting agency code, bureau code, mission area (where appropriate), part of the exhibit where investment will be reported, type of investment, agency four-digit identifier, and two-digit investment category code. Details are provided in section 53.9.

- ***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 could include impacted UPIs, reference to legislation, or governance board decision dates.

- ***Agency Funding*** is the agency's funding authority for a given investment.

- ***Business Solutions*** are comprised of software application, systems, services and the people, processes, commercial contracts, overhead occupancy, and technology that are used to acquire, manage, manipulate, display and compile information and data in direct support of the mission of the Department. Agencies should not duplicate costs for Infrastructure when accounting for business solutions.

- ***Change in Investment Status*** is used when an investment in PY or CY portfolio has a change in status (i.e. downgraded to non-major, eliminated, retired, consolidated, split) for the CY or BY. The change of status should be indicated with one of the following reasons: 1) Downgraded to non-major because it does not fit the criteria for Major investment in FY 2012, or because of insufficient activities or funding, 2) In FY 2012 this consolidated investment is no longer included in Major Investments, due to the split up into separate component investments 3) In FY 2012 this investment is no longer a major investment, due to consolidation of activities into another investment 4) Investment was subject to agency-wide realignment of the IT portfolio, 5) Investment was retired, 6) Investment was eliminated or 7) Upgraded to Major Investment, 8) Other, 0)None.

- ***Contributions (Expected Contributions)*** would include 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.

- ***Core Financial System Percentage*** means the portion of this investment's funding associated with the core financial system of record that maintains all transactions resulting from financial events.

- ***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.

- ***Data Center Consolidation Plan*** identifies potential areas for consolidation, areas where optimization through server virtualization or cloud computing alternatives may be used, and a high-level roadmap for transitioning to the consolidated end-state architecture.

- ***Data.gov Integration*** means an IT investment that creates value by publishing data sets through Data.gov as described in the Data.gov Concept of Operations. Specifically, value is created by publishing data sets that 1) drive market participant accountability by describing participant behavior or attributes; 2) enable information-centric markets by ensuring producers and consumers have the maximum appropriate information to inform their purchase decisions; 3) support Federal accountability by revealing the results and characteristics of government services to citizens; 4) improve government efficiency and effectiveness by releasing information about how Federal agencies conduct financial management or manage resources; and 5) promote the connected citizen by sharing information about the policy, rulemaking, and public engagement process; 0) none, the investment does not publish data through Data.gov. If the investment uses or publishes data through Data.gov, indicate the targeted value creation mode by listing the corresponding number.

- ***Development/Modernization/Enhancement (DME)*** means the program cost for new investments, changes or modifications to existing systems to improve capability or performance, changes mandated by the Congress or agency leadership, personnel costs for investment management, and direct support. For major IT investments, this amount should equal the sum of amounts reported for planning and acquisition plus the associated FTE costs reported in the exhibit 300.

- ***End User Systems and Support***—End user hardware (desktop, laptop, and handheld devices), peripherals (local printers, shared printers, and scanners), and software (PC operating systems, office automation suites, messaging and groupware), and hardware and software for help desks.

- ***Funding Source*** means any budgetary resource used for funding the IT investment. Budgetary resource is defined in section 20. 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."

- ***Funding Source Subtotal*** represents the total of all funding source line items used for funding a particular IT investment.

- ***Homeland Security Presidential Directive-12 (HSPD-12)*** means the amount of this investment's PY/2010 funding associated with the agency's HSPD-12 implementation.

- ***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.

- ***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 Technology Practices and Management*** are programmatic and service costs of the people, processes, commercial contracts, overhead occupancy, technology and services. Examples of costs to be reported include: Enterprise architecture program costs, investment management program costs, and other IT management costs.

- ***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 UPI). 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 UPI of the managing partner's business case (i.e. managing partner UPI).

- ***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).

- ***Mainframes and Servers Services and Support*** Mainframes and servers [including web hosting (but not Web content development and management)] hardware and software operations, licenses, maintenance, back-up, continuity of operations, and disaster recovery. Also includes electronic messaging and storage. Includes data center and data center system components including, mainframe mid-tier systems, servers, storage, as well as all the component systems used to house the data center equipment in environmentally correct conditions, including UPS, back-up generators, HVAC systems, and building management systems.

- ***Primary FEA Mapping—BRM Line of Business*** means the 3-digit code for the primary Line of Business from the FEA BRM. This is required for all investments. BRM Line of Business codes can be found at http://www.egov.gov. Note: The BRM Mode of Delivery lines of business are not valid for Primary FEA Mappings.

- ***Primary FEA Mapping—BRM Sub-Function*** means the 3-digit code for the primary Sub-function under the BRM Line of Business identified in the BRM Line of Business. This is required for all investments. BRM Sub-function codes can be found at http://www.egov.gov. Note: The BRM Mode of Delivery sub-functions are not valid for Primary FEA Mappings.

- ***Segment Architecture*** represents the identifier depicting the agency segment as well as the standard segment the investment supports. The six digit segment code entered on the Exhibit 53 must match a segment code coordinated and maintained by the agency Chief Architect and registered with the FEA PMO. Details are provided in section 53.9.

- ***Steady State (SS)*** means maintenance and operation costs at current capability and performance level including costs for personnel, maintenance of existing information systems, corrective software maintenance, voice and data communications maintenance, and replacement of broken IT equipment. For major IT investments, this amount should equal the amount reported for maintenance plus the associated FTE costs reported in the exhibit 300.

- ***Supports Information Sharing and Access*** means an IT investment supporting the information sharing and access mission areas of 1) the national network of State and major urban area fusion centers, 2) Interoperability across Sensitive but Unclassified Networks targeting federal, state, local, and tribal law enforcement, public safety, homeland security, and intelligence personnel, 3) Classified National Security Information Program for State, local, tribal, and private sector partners, 4) National Suspicious Activity Reporting Initiative, and 5) Controlled Unclassified

Information, or 0) none. If the investment supports one of these mission areas, indicate which one(s) by listing the corresponding number(s) listed above.

- ***Telecommunications Systems and Support***—Telecommunications (including wireless, multimedia, and local and long distance telephone) hardware and software operations, licenses, maintenance, back-up, continuity of operations, and disaster recovery. Also includes network operations command centers, wire closets and cable management.

(b) ***Part 1. IT investments for Mission Area Support***

Consistent with your agency's strategic and annual performance plan, report amounts for IT investments directly supporting an agency-designated mission area (e.g., human resource management, financial management, command and control). Report each mission area in which IT investments are funded, itemizing the "major" and "non-major" IT investments within each mission area.

Agencies must have a mission area titled "Financial Management", and it must be reported as the first mission area. Some IT investments support financial functions in addition to other functions. If an IT investment supports financial functions, you must include an estimated percentage of the total IT investment obligations associated with the core financial system components. Use the financial operations and core financial system definitions provided in this section for a description of functions relevant for determining the percent of core system costs. While budget formulation and execution systems are part of Financial Management, they are not included in this percent estimation of the core financial system. If the IT investment reported is 100 percent core financial, indicate "100" percent in the column. For mixed systems, indicate the appropriate percentage that is the core financial system.

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

Report all IT investments primarily supporting common user systems, security, communications, and computing infrastructure. 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 may involve multiple mission areas and include End User Systems, Mainframes and Servers, and Telecommunications. It includes both 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 management costs.

Agencies are encouraged to report these investments as they are managed. Thus, if infrastructure is managed bureau by bureau, then bureau-level infrastructure investments should be listed.

Report your IT security initiatives and investments not directly tied to a major investment on a separate line identified as "non-major."

(d) ***Part 3. IT investments for Enterprise Architecture and Planning***

Report amounts for IT investments supporting strategic management of IT operations (e.g., business process redesign efforts not part of an individual investment or initiative, enterprise architecture development, capital planning and investment control processes, procurement management, and IT policy development and implementation).

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

Report amounts for IT investments representing planning, developing, enhancing or implementing a grants management system or portion thereof. Include any grants systems initiatives.

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

Report amounts for IT investments representing planning, development, enhancements or implementations 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, enhancements or implementations 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 OMB representative.

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):

- ***Agency Code***—3 digit agency identifier
- ***Anti-Virus***—a program that monitors desktops/laptops to identify all major types of viruses and prevents or contain virus incidents.
- ***Anti-Malware***—a program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.
- ***NIST 800-37 implementation activities-*** activities defined in OMB Circular A-130, Appendix III and NIST Special Publication 800-37.
- ***Data leakage protection tools***—systems designed to detect and prevent the unauthorized use and transmission of confidential information including encryption for PII.
- ***Email Filtering Software***—software that organizes e-mail according to defined criteria, most commonly used for detecting and eliminating spam and malware.
- ***FISMA annual testing***—testing required under the Federal Information Security Management Act of 2002 (FISMA), other than testing conducted as part of the certification accreditation. It does not include costs for annual disaster recovery and contingency plan tests. It does cover annual security controls testing.
- ***Intrusion Detection System (IDS)***—software that looks for suspicious activity on networks and alerts administrators.
- ***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.
- ***Network Penetration Testing***—method of evaluating the security of computer networks by simulating attach by a hostile actor.
- ***Security Awareness Training***—annual training required under FISMA for all employees, contractors and other people with log-in privileges to an agency's networks.
- ***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.

- ***Security Training for people with significant security responsibilities*—**training required by FISMA for government employees with significant security responsibilities. Please refer to NIST Special Publication 800-16.

- ***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 17 digit line number coding system to update or complete your exhibit 53 (Each investment identified in the agency's portfolio must have a unique UPI):

Entry	Description
XXX–xx–xx–xx–xx–xxxx–xx	The first three digits are your agency code (see Appendix C).
xxx–XX–xx–xx–xx–xxxx–xx	The next two digits are your bureau code (see Appendix C). If this is a department only reporting or an agency-wide activity, use 00 as your bureau code.
xxx–xx–XX–xx–xx–xxxx–xx	These two digits indicate the six parts of the exhibit 53: 01 = Part 1. IT investments for Mission Area Support 02 = Part 2. IT investments for Infrastructure, IT Security, Office Automation, and Telecommunications 03 = Part 3. IT Investments for Enterprise Architecture and Planning 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
xxx–xx–xx–XX–xx–xxxx–xx	These two digits indicate the mission area. Assign a unique code for each mission area reported.
xxx–xx–xx–xx–XX–xxxx–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 53.3) 02 = Non-major IT investments (see definition in section 53.3) 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.
xxx–xx–xx–xx–xx–XXXX–xx	This is a four-digit identification number to identify a specific IT investment. If a new investment is added to exhibit 53, locate the area of exhibit 53 where you are going to report the IT investment and use the next sequential number as your four digit identification number. To avoid duplicative UPIs, review agency's portfolio before finalizing this identification number for new or updated investments.

Entry	Description
xxx–xx–xx–xx–xx–xxxx–XX	These two digits identify the investment category of the investment you are reporting. Select one of the following two digit codes according to what you report on the title line: 00 = Total investment title line, or the first time the agency is reporting this particular investment. 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. 04 = Funding source or appropriation 09 = Any subtotal

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).
xxx–XX–xxxx–x	The next two digits are your bureau code (see Appendix C).
xxx–xx–XXXX-x	This is a four-digit Account Symbol for the appropriate MAX Account. (see section 79.2)
xxx–xx–xxxx-X	This is a single digit Transmittal Code. (see section 79.2, and note on ARRA funding in section 53.7)

Use the following 6 digit number coding system to identify each investment's 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: 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

Entry	Description
	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 section 53.4 and 53.8 for definitions.

AGENCY IT INVESTMENT PORTFOLIO

Entry	Description
Part 1. IT investments for Mission Area Support	Report IT investments that directly support an agency-designated mission area. Report each mission 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 area 01 is reserved for your "core financial system" IT investments. Step 1: For each mission area, list each major IT investment and the corresponding investment costs. If a system in BY is financial or mixed, identify what percentage of funding relates to its functions as a core financial system in BY. 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 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. These investments are encouraged to 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, Mainframes and Servers, and Telecommunications. All IT Investments capturing shared services are to be included in Part 2.
Part 3. IT Investments for Enterprise Architecture and Planning	Each agency should list all enterprise architecture efforts. For the President's Budget, enterprise architecture 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 the investments' UPI codes 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, 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 UPI (17–digits required for all)
Column 3: Change in Investment Status Identifier (1 digit code)
Column 4: Agency description of change in investment status (limited to 255 characters)
Column 5: Investment Title
Column 6: Investment Description (limited to 255 characters)
Column 7: Primary FEA Mapping—Line of Business (3 digit code)
Column 8: Primary FEA Mapping—Sub-Function (3 digit code)
Column 9: Core financial system (%)
Column 10: HSPD-12 ($M)
Column 11: Homeland Security Priority Identifier (select all that apply)
Column 12: Is this investment accounted for in the agency Data Center Consolidation Plan (yes/no)
Column 13: Cross-Boundary Information Sharing Identifier (1 digit code)
Column 14: Supports Information Sharing and Access (select all that apply)
Column 15: Data.gov Integration Identifier (1 digit code)
Column 16: Development, Modernization, Enhancement (DME) (PY/2010) Agency Funding($M)
Column 17: Development, Modernization, Enhancement (DME) (PY/2010) Contributions ($M)
Column 18: Development, Modernization, Enhancement (DME) (CY/2011) Agency Funding ($M)
Column 19: Development, Modernization, Enhancement (DME) (CY/2011) Expected Contributions ($M)
Column 20: Development, Modernization, Enhancement (DME) (BY/2012) Infrastructure, EUSS ($M)
Column 21: Development, Modernization, Enhancement (DME) (BY/2012) Infrastructure MSSS ($M)
Column 22: Development, Modernization, Enhancement (DME) (BY/2012) Infrastructure TSS ($M)
Column 23: Development, Modernization, Enhancement (DME) (BY/2012) IT Security ($M)
Column 24: Development, Modernization, Enhancement (DME) (BY/2012) Other, Business Solutions, and IT Practices and Management ($M)
Column 25: Development, Modernization, Enhancement (DME) (BY/2012) Total ($M) = sum of columns 20-24
Column 26: Steady State (SS) (PY/2010) Agency Funding($M)
Column 27: Steady State (SS) (PY/2010) Contributions ($M)
Column 28: Steady State (SS) (CY/2011) Agency Funding ($M)
Column 29: Steady State (SS) (CY/2011) Expected Contributions ($M)
Column 30: Steady State (SS) (BY/2012) Infrastructure, EUSS ($M)
Column 31: Steady State (SS) (BY/2012) Infrastructure MSSS ($M)
Column 32: Steady State (SS) (BY/2012) Infrastructure TSS ($M)
Column 33: Steady State (SS) (BY/2012) IT Security ($M)
Column 34: Steady State (SS) (BY/2012) Other, Business Solutions, and IT Practices and Management ($M)
Column 35: Steady State (SS) (BY/2012) Total ($M) = sum of columns 30-34
Column 36: Segment Architecture (6 digit code)

For the BY, investment costs should be represented in a minimum of one of the following columns: 20-24 and 30-34. Agencies unable to provide the BY break-out by funding source should provide this information at the investment line, at a minimum.

AGENCY IT SECURITY PORTFOLIO

	Row	Description
1	Agency Code	Three digit agency identifier (see Appendix C)
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	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	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 Costs	This row is calculated by adding Rows 6-13, IT Security software and tools licensing costs.
7	Anti-Virus Software Licensing Costs	Report 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. 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.
8	Anti-Malware Software Licensing Costs	Report 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.
9	Intrusion Detection Systems Licensing Costs	Report 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. 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.
10	Intrusion Prevention Systems Licensing Costs	Report 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.
11	Web Filtering Software Licensing Costs	Report 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.
12	Email Filtering Software	Report 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. Costs should be reported in thousands and reported to the dollar.
13	SIM/SIEM tools	Report the tool costs incurred or expected to be incurred for the respective budget year. Costs should be reported in thousands and reported to the dollar.
14	Data Leakage	Report the tool costs incurred or expected to be incurred for the respective

	Row	Description
	Protection tools	budget year. Costs should be reported in thousands and reported to the dollar.
15	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. Certification and Accreditation costs should only include contract costs.
16	Number of systems scheduled for activities represented in Row 15.	Number of systems used to in cost calculations for "Costs for NIST 800-37"
17	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.
18	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
19	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.
20	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 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
Row 4: Number of contractor FTEs with information security responsibilities
Row 5: Average cost per contractor FTE
Row 6: (calculated) Total IT Security Tools Costs
Row 7: Anti-virus software
Row 8: Anti-malware software
Row 9: Intrusion detection systems
Row 10: Intrusion prevention systems
Row 11: Web filtering software
Row 12: Email filtering software
Row 13: SIM/SIEM tools
Row 14: Data leakage protection tools
Row 15: Costs for implementation and activities associated with NIST 800-37 of systems
Row 16: Number of systems scheduled for the activities represented in Row 15.
Row 17: Annual FISMA testing costs
Row 18: Network penetration testing activities costs
Row 19: Security awareness training costs
Row 20: Security training costs for employees with significant security responsibilities