NIST Special Publication 800-65, Revision 1(Draft)

Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process (Draft)

Pauline Bowen
Richard Kissel
Matthew Scholl
Will Robinson
Jessica Stansfield
Lisa Voldish

National Institute of Standards and Technology • U.S. Department of Commerce

NIST Special Publication 800-65, Revision 1 (Draft)

Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process (Draft)

Pauline Bowen
Richard Kissel
Matthew Scholl
Will Robinson
Jessica Stansfield
Lisa Voldish

July, 2009

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Deputy Director

National Institute of Standards and Technology Special Publication 800-65, Revision 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-65, Revision 1, 56 pages (July, 2009)
CODEN: NSPUE2

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

Acknowledgements

TBD

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Executive Summary

Traditionally, information security and capital planning have been treated as separate activities by security and capital planning practitioners. However, with Federal Information System Management Act (FISMA) legislation, existing federal regulations that charge agencies with integrating the two activities. Additionally, with increased competition for limited federal budgets, agencies must effectively integrate their information security and capital planning processes. This guidance discusses how information security considerations, including continuous monitoring, Plans of Action and Milestones (POA&M), external evaluations, new mandates, evolving threats, and system life cycle considerations impact capital planning considerations. This guidance also discusses considerations and frameworks agencies can use to prioritize security investments and help ensure that security concerns are incorporated into the capital planning process to deliver maximum security and mission value to the agency.

As defined by the Clinger Cohen Act and OMB Circular A-11, Capital Planning and Investment Control (CPIC) 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 CPIC process consists of three phases: Select, Control, and Evaluate:

- The Select phase refers to activities associated with assessing and prioritizing current and proposed IT projects based on mission needs and improvement priorities. Typical Select phase activities include screening new projects; analyzing and ranking all projects based on benefit, cost, and risk criteria; selecting a portfolio of projects; and establishing project review schedules.

- The Control phase refers to activities designated to monitor the investment during its operational phase to determine if the investment is within the cost and schedule milestones established at the beginning of the investment life cycle.

- The Evaluate phase determines how well the investment is delivering expected results. The Evaluate phase addresses the question, "Did the investment achieve the desired results and performance goals identified during the Select phase?"

Information security is an important element in the planning, acquisition and management of federal information systems. Information security drivers impact an investment's business requirements and must be addressed throughout the Select, Control and Evaluate life cycle phases. Planning for information security is strategically important to ensure that the investment is adequately funded to satisfy information security requirements and that cost-effective security controls are in place to meet information security requirements and to protect the investment's information assets.

Agencies have numerous security considerations competing for funding. Security considerations may be:

- New – e.g., a new system, a new release of an existing system or a new mandate;

- Existing – e.g., maintenance activities such as annually testing security controls or conducting a recertification; or,

- Corrective – e.g., POA&M corrective actions.

One option agencies can use to prioritize security requirements is to use criteria and weighting factors to rank security requirements through a risk-based prioritization. Based on the output, agencies may decide which security requirements should be addressed immediately and funded through the current operating budget; which security requirements may be delayed and seek new funding through the budget request; and which security requirements will not be funded and the residual risk will be accepted.

While specific inputs will vary slightly from organization to organization, typical inputs to agency information security investment decision making include:

- Continuous monitoring results;
- Vulnerabilities and associated corrective actions/remediation activities logged into POA&Ms;
- Vulnerabilities and associated corrective actions/remediation activities identified in external evaluations (e.g., General Accountability Office [GAO] and Inspector General [IG] audits and analyses);
- New mandates (e.g., OMB mandates, which are often unfunded);
- Evolving threats, such as zero-day exploits, incidents, warnings and bulletins from United States Computer Emergency Readiness Team (US-CERT), and other associated threats; and,
- Other organization-specific activities.

Once security considerations have been identified, agencies must determine which considerations should be implemented. Funding and resources are not always available to cover all security needs, therefore considerations must be prioritized to address the most pressing security needs first and to ensure the most effective use of resources. To effectively prioritize security considerations, agencies must identify criteria for prioritization.

Once agency management and stakeholders agree on prioritization requirements, the agency must begin the ranking process by assessing the security considerations against the prioritization criteria. Each security consideration is assigned a quantitative value that represents the consideration's ability to meet the intent of the criterion. Once all security considerations have received an assessment for each criterion, the assessment value is multiplied against the criterion weight. All weighted values are then added together to obtain a total score for the security consideration. The total scores may then be compared to rank-order the security considerations.

Security considerations with the highest score represent the top priority or most critical security investments. The objective is to apply the first security dollar to the most critical security investment. The next dollar is then applied to the next critical security investment and so forth until the security budget is expended.

The process presented in this guidance is intended to serve as a model methodology. Agencies should work within their investment planning environments to adapt and incorporate the pieces of this process into their own unique processes to develop workable approaches for CPIC. If incorporated into an agency's processes, the methodology can help ensure that IT security is appropriately planned for and funded throughout the investment's life cycle, thus strengthening the agency's overall security posture.

1. Introduction

1.1 Background

With the release of the Federal Information Security Management Act (FISMA) in 2002, the need for information security guidance within the federal community has increased. Capital planning was once seen as applying primarily to large-scale information systems. However, laws and requirements now drive the integration of information security and capital planning, for example:

- FISMA places emphasis on information security at both the system and enterprise levels, and links information security to capital planning;[1]
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, requires specific security considerations throughout the investment life cycle; and,
- OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*, requires agencies to plan for and track direct and indirect Information Technology (IT) security costs throughout the investment life cycle.

As a prerequisite for receiving budget allocations, information security investments must be accounted for in the Capital Planning and Investment Control (CPIC) process. The CPIC process 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 purpose of the process is to ensure that all IT investments directly support and align with the Department's mission and strategic goals, and that all IT investments support business needs, while minimizing risks and maximizing value. CPIC is synonymous with capital programming. This guidance focuses on risk minimization in the CPIC process through sound, risk-based security planning, and decision-making practices.

Traditionally, information security and capital planning have been treated as separate activities by security and capital planning practitioners. However, with FISMA legislation, existing federal regulations that charge agencies with integrating the two activities, and increased competition for limited federal budgets, agencies must effectively integrate their information security and capital planning processes. This guidance discusses how information security considerations, including continuous monitoring, Plans of Actions and Milestones (POA&M), external evaluations, new mandates, evolving threats, and system life cycle considerations impact capital planning considerations. This guidance also discusses considerations and frameworks agencies can use to prioritize security investments and help ensure that security concerns are incorporated into the capital planning process to deliver maximum security and mission value to the agency.

This special publication was developed under the assumption that the reader possesses a basic familiarity with requisite information security and capital planning guidance and legislation including FISMA, OMB Circulars A-11 and A-130, the Clinger-Cohen Act, NIST special publications, and is familiar with security controls and requirements.

[1] FISMA requires weaknesses and vulnerabilities to be tracked and remediated. This process is usually accomplished through the Plan of Action and Milestones (POA&M) process which ties resources to weakness remediation activities.

1.2 Relationship to Existing Guidance

This document is a continuation in a series of NIST special publications (SP) intended to assist information security personnel in planning and prioritizing their information security investments.[2] NIST SP 800-55, Rev. 1, *Performance Measurement Guide for Information Security*, can be used in conjunction with continuous monitoring as a source for baselining an agency's information security posture and identifying areas for future security investments. NIST SP 800-55 Rev. 1 also provides processes and example measures that can be used to support creation of the artifacts required to integrate information security into the CPIC process.

Furthermore, NIST SP 800-64, Rev. 2, *Security Considerations in the System Development Life Cycle*, discusses key security requirements throughout the System Development Life Cycle (SDLC) that require forethought and budget allocations to successfully implement. Agencies can use the capital planning strategies discussed in this guidance document to ensure they have the plans and budget in place to implement the appropriate security activities throughout the SDLC.

This document contains several references to OMB guidance, including OMB Circular A-11. This document intends to provide notional strategies for providing security inputs to the capital planning process. This guidance does not supersede Circular A-11; rather, it provides additional information to assist agencies with successfully integrating information security into their capital planning processes.

1.3 Purpose and Scope

This document can be used to assist federal agencies in integrating information security into their CPIC processes by providing guidance on selecting, managing, and evaluating information security investments and accounting for information security in all IT investments. This guidance will explain the relationships between CPIC, Enterprise Architecture (EA), and organizational security programs.

The guidance will assist federal information security practitioners to:

- Articulate the need to integrate the security, risk-based decision making, and capital planning processes;
- Identify relevant OMB and other guidance that applies to governing federal government information security investment decisions;
- Explain how current information security requirements relate to and support the IT CPIC process;
- Understand the IT investment management process phases—Select, Control, and Evaluate—as they relate to information security investments;
- Identify CPIC-related roles and responsibilities required to manage IT investments;
- Understand how to develop security requirements and appropriate supporting documentation for IT acquisition and weakness remediation;
- Identify steps and materials required to complete a sound business case in support of investment requests; and,

[2] This document also relies on the material presented in the following NIST Special Publications:

- Draft NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, contains information on agency-level security requirements and prioritization activities;
- Draft NIST SP 800-37, Rev. 1, *Guide for Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, is a key source of security capital planning requirements; and,
- Draft NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems*, provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government.

- Understand implementation issues associated with incorporating information security into the CPIC process.

1.4 Security Capital Planning and Investment Control Process Overview

As defined by the Clinger Cohen Act and OMB Circular A-11, CPIC 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.[3] The purpose of the process is to ensure that all IT investments directly support and align with an agency's mission and strategic goals, and that all IT investments support business needs, while minimizing risks and maximizing value. CPIC is synonymous with capital programming.

Agencies have numerous security requirements competing for funding. One option agencies can use to prioritize security requirements is to use criteria and weighting factors to rank security requirements through a risk-based prioritization. Based on the output, agencies may decide which security requirements should be addressed immediately and funded through the current operating budget; which security requirements may be delayed and seek new funding through the budget request; and which security requirements will not be funded and the residual risk will be accepted.

One avenue agencies may pursue for obtaining new funding for security requirements is through the federal budget process. Additional funding may be obtained by increasing the budget request for an existing IT investment or adding a new investment to the agency's IT Investment Portfolio. The investments reported in the agency's IT Investment Portfolio are selected and managed through the CPIC process. Though the CPIC process is not the only means for obtaining funding for IT initiatives, it is the focus of this document.

It should be noted that investments approved through the CPIC process are not guaranteed funding. Once an investment has been selected, it becomes a part of the agency's IT Investment Portfolio and is listed in the agency's Exhibit 53. The Exhibit 53 represents the agency's entire IT budget request. Agencies submit their Exhibit 53 to OMB each September and the information is used to prepare the President's budget. Congress reviews the President's budget, holds hearings to evaluate the budget proposal and approves the appropriations bills. Once the president signs each of the appropriations bills into law, the budget is enacted.

After the budget is enacted, OMB appropriates funds to each agency. It is the agency's responsibility to control the use of those funds. Each agency develops an operating plan and the agency's senior leadership allots funding to agency programs. The amount of funding each IT investment receives will be impacted by resources made available in the appropriations act, Congressional concerns, and the agency's priorities.

1.5 Definitions

This section will contain definitions to any key terms that are essential to understanding the integration of IT security into the capital planning process. Key definitions include:

- ***Capital Planning and Investment Control (CPIC)*** 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 purpose of the process is to ensure that all IT investments directly support and align with the Department's mission and strategic goals, and that all IT investments support business needs, while minimizing risks and maximizing returns.[4]

[3] Definition from OMB Circular A-11, Part 2, Preparation and Submission of Budget Estimates
[4] Clinger Cohen Act of 1996

- ***Security controls*** are the management, operational, and technical controls (*i.e.*, safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.[5]

- An ***IT security investment*** is an IT application, service or system that is solely devoted to security. For instance, intrusion detection systems (IDS) and public key infrastructure (PKI) are examples of IT security investments.

- Security risk versus investment risk are two distinctly different measures:

  - **Security risk**. The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.[6]

  - **Investment risk**. Risks associated with the potential inability to achieve overall program objectives within defined cost, schedule, and technical constraints.

- Select-Control-Evaluate[7] is an IT investment management process:

  - **Select**. The goal of the selection phase is to assess and prioritize current and proposed IT projects and then create a portfolio of IT projects. In doing so, this phase helps to ensure that the organization (1) selects those IT projects that will best support mission needs and (2) identifies and analyzes a project's risks and returns before spending a significant amount of project funds. A critical element of this phase is that a group of senior executives makes project selection and prioritization decisions based on a consistent set of decision criteria that compares costs, benefits, risks, and potential returns of the various IT projects.

  - **Control**. The control phase consists of managing investments while monitoring for results. Once the IT projects have been selected, senior executives periodically assess the progress of the projects against their projected cost, scheduled milestones, and expected mission benefits.

  - **Evaluate**. The evaluation phase provides a mechanism for constantly improving the organization's IT investment process. The goal of this phase is to measure, analyze, and record results based on the data collected throughout each phase. Senior executives assess the degree to which each project has met its planned cost and schedule goals and has fulfilled its projected contribution to the organization's mission. The primary tool in this phase is the post-implementation review (PIR), which should be conducted once a project has been completed. PIRs help senior managers assess whether a project's proposed benefits were achieved and also help to refine the IT selection criteria to be used in the future.

1.6 Audience

The audience for this document includes executive management, IT managers and information security professionals, security program managers, Investment Review Board (IRB) participants, and other financial and budget personnel.

[5] NIST SP 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*.
[6] NIST SP 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*
[7] The Select, Control, and Evaluate framework was produced cooperatively by OMB's Office of Information and Regulatory Affairs and the GAO's Accounting and Information Management Division. Source – OMB's Guidance: Evaluating Information Technology Investments, A Practical Guide, Version 1, Office of Information and Regulatory Affairs, Information Policy and Technology Branch, November 1995.

1.7 Document Organization

The remaining sections of this guide discuss the following:

- Section 2, Capital Planning and Security Planning Environment Overview, provides an overview of capital planning, information security management planning, enterprise architecture, inventory consistency, and timelines associated with capital plans and budget cycles.
- Section 3, Integration of Security and the Capital Planning and Investment Control Process, describes the integration of IT security into the CPIC process.
- Appendix A contains a glossary of terms used in the document.
- Appendix B lists the references used in the document.
- Appendix C lists legislation, regulation, and guidance related to capital planning and information security.
- Appendix D provides guidance on how to address the security section of the OMB Exhibit 300.
- Appendix E provides an example of how the guidance presented in this document may be implemented to select and fund security considerations.

2. Capital Planning and Security Planning Environment Overview

2.1 Capital Planning Overview

The Clinger-Cohen Act of 1996 requires agencies to use a disciplined CPIC process to acquire, use, maintain and dispose of information technology. Specifically, the Clinger Cohen Act requires agencies to develop CPIC processes that:

- Integrate processes for selection, management and evaluation of IT investments with budget, financial, and program management decisions;
- Include minimum criteria for investment decisions and quantifiable measurements for determining net benefits and risks;
- Identify investments that would result in shared benefits or costs for federal agencies or state or local governments; and,
- Provide senior management with timely information (cost, effectiveness, timeliness and quality).

CPIC accomplishes these requirements through three distinct phases: Select, Control, and Evaluate. Each stage of the CPIC process is integral to ensuring that investments are appropriately managed throughout their life cycle.

The Select phase refers to activities associated with assessing and prioritizing current and proposed IT projects based on mission needs and improvement priorities. Typical Select phase activities include screening new projects; analyzing and ranking all projects based on benefit, cost, and risk criteria; selecting a portfolio of projects; and establishing project review schedules. A project approved in the Select Phase becomes part of the agency's IT portfolio, which is submitted to OMB for inclusion in the President's budget.

The Control phase refers to activities designated to monitor the investment during its operational phase to determine if the investment is within the cost and schedule milestones established at the beginning of the investment life cycle. Typical processes involved in the Control phase include using a set of performance measures to monitor the developmental progress for each IT project to enable early problem identification and resolution.

After the investment has become operational, the Evaluate phase determines how well the investment is delivering expected results. The Evaluate phase addresses the question, "Did the investment achieve the desired results and performance goals identified during the Select phase?"

OMB Circular A-11 provides the requirements for the formulation and execution of the federal budget. Part 2, Section 53 and Part 7, Section 300 of the Circular address the requirements for reporting IT spending. Part 2, Section 53 requires agencies to report all IT investments in their Exhibit 53 submission. The investments reported in the Exhibit 53 are identified through the Select Phase and are referred to as the agency's IT Investment Portfolio. Federal agencies report their IT Investment Portfolio annually to OMB. The Exhibit 53 provides OMB with a summary view of the IT investments in an agency's portfolio and is used by OMB to create an overall "Federal IT Investment Portfolio," which is published as part of the President's budget.

In addition to the Exhibit 53, Part 7, Section 300 requires agencies to submit an Exhibit 300 for all major IT investments. OMB defines a major investment as 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.[8]

In addition to the criteria defined by OMB in Circular A-11, each agency sets specific criteria to identify a major investment. One criterion that many agencies include in the criteria is a dollar threshold. Specific thresholds vary from agency to agency.

2.2 Information Security Management Planning

FISMA requires agencies to integrate information security into their capital planning process, conduct annual information security review of all programs and systems, and report the results of those reviews to OMB. Additionally, agencies can integrate the results of their information security and capital planning processes into their EA process to promote a coordinated approach to achieving mission and business goals.

Information security is an important element in the planning, acquisition and management of federal information systems. Information security drivers impact an investment's business requirements and must be addressed throughout the Select, Control and Evaluate life cycle phases. Planning for information security is strategically important to ensure (a) the investment is adequately funded to satisfy information security requirements and (b) that cost-effective security controls are in place to meet information security requirements and to protect the investment's information assets.

Information security investments may occur at the enterprise level or system level:

- Enterprise-level investments – funding for those information security investments that are ubiquitous across the agency and will improve the overall agency's security posture. Examples of these type of investments include an enterprise-wide firewall, IDS acquisition, PKI, or an initiative to address program security weaknesses.
- System-level investments – funding for the management, operational and technical controls of a specific information system. Examples include Certification and Accreditation (C&A), testing an IT Contingency Plan (ITCP) or correcting a system-level security weakness.

Information security and privacy are crucial components of the CPIC process, as specific security and privacy activities take place during each stage of an investment's life cycle. Figure 2-1 depicts information security activities throughout the Select, Control, and Evaluate phases.

[8] Definition from OMB Circular A-11, Part 2, Preparation and Submission of Budget Estimates

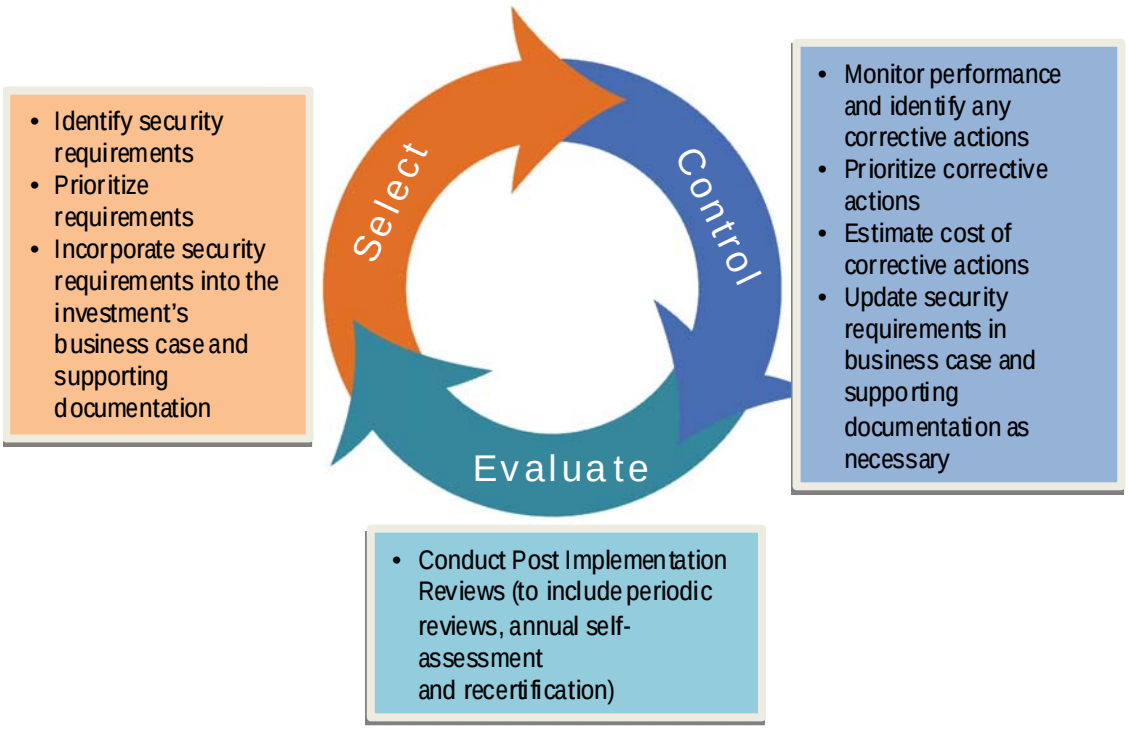

Figure 2-1. Security Considerations Throughout the CPIC Process

Key activities and decisions take place throughout the CPIC process to ensure that security requirements are identified, planned for and implemented as a part of an individual IT investment or the overall agency investment portfolio. During the Select phase, information security drivers include assessment activities to ensure that information security investments comply with information security requirements. During the Control phase, investments are monitored through the use of security metrics to ensure that security controls are in place and operational; corrective actions are identified. During the Evaluate phase, security drivers include self-assessment activities to ensure investments remain compliant with requirements

2.3 Enterprise Architecture

EA is a management practice that aims to maximize the contribution of an organization's resources to achieve mission/business success. Architecture can establish a clear line of sight from investments to measurable performance improvements whether for the entire enterprise or a portion (or segment) of the enterprise. EA provides a common language for discussing information security with regard to mission/business processes and performance goals, enabling better coordination and integration of efforts and investments across organizational or business activity boundaries. For the federal government, the Federal Enterprise Architecture (FEA) [9] defines a collection of interrelated reference models including Performance, Business, Service Component, Data, and Technical as well as more detailed segment and solution architectures that are derived from the top-level EA. Organizational assets (including programs, processes, information, applications, technology, investments, personnel, and facilities) are mapped to the enterprise-level reference models to create a segment-oriented view of the enterprise. Segments, defined by the EA, are individual elements of the enterprise describing core mission areas, and common or shared business services and enterprise services. From an investment perspective, segment architecture drives

[9] The Federal Enterprise Architecture is described in a series of documents published by the OMB FEA Program Management Office. www.whitehouse.gov/omb/e-gov

decisions for a business case or group of business cases supporting a core mission area or common or shared service. The primary stakeholders for segment architectures are mission/business owners and managers. These stakeholders, in consultation with the Senior Agency Information Security Officer (SAISO) should incorporate information security requirements from the FISMA legislation and associated NIST security standards and guidelines into the segment architecture to provide appropriate levels of protection for the organization's mission and business processes defined as part of the overall EA.

Solution architecture defines the organization's IT assets such as applications or information system components used to automate and improve individual organizational mission/business processes. The scope of an organization's solution architecture is typically used to implement all or part of an information system or business solution. The primary stakeholders for solution architectures are information system developers and users. Security requirements defined in an organization's segment architecture are allocated in the form of specific security controls to individual information systems (and components composing those systems), through the solution architecture. To summarize, information security considerations can be addressed as an integral part of the EA by:

- Developing segment architectures to support clear and concise value propositions linked to organizational missions and strategic goals and objectives;
- Identifying where information security is a critical element in mission/business processes, information, applications, or technologies in use within organization-defined segments;
- Defining information security requirements and risk mitigation strategies to provide adequate protection for the mission/business processes, information, applications, or technologies within segments based on the organization's tolerance for risk (i.e., risk/reward ratio);
- Translating information security requirements and risk mitigation measures from the segment architecture into security controls for information systems and system components as part of solution architectures;
- Allocating specific security controls to individual information system components defined within solution architectures; and,
- Documenting risk management decisions at all levels of the EA. [10]

To achieve target performance improvements the EA practice must be fully integrated with other practice areas including strategic planning, CPIC, and program and project management.[11] The security categorization that begins the security life cycle is a business-enabling activity directly feeding the EA and CPIC processes for new investments, as well as migration and upgrade decisions. It can provide a firm basis for justifying certain capital expenditures and also can provide analytical input to avoid unnecessary investments.[12]

Agencies typically maintain two versions of their EA. The version that portrays the existing enterprise, the current business practices and the associated technical infrastructure is defined as a baseline or as-is architecture. The as-is architecture can be used to reduce costs and increase interoperability by helping organizations become aware of and reuse existing assets and develop enterprise solutions with reuse and interoperability in mind. Understanding and establishing reusable components is an integral part of continuously improving an organization's IT portfolio management. EA also describes the desired future state for an organization—called the target or to-be architecture. Like the as-is architecture, the to-be

[10] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*
[11] FEA Practice Guidance, November 2007, Federal Enterprise Architecture Program Management Office, OMB.
[12] NIST SP 800-60 Volume I, Revision 1, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*

architecture defines business objectives and supportive activities in both business and technical terms. Organizations move from the baseline state to the target state through a transition plan.

The enterprise architecture transition plan should include clear linkage between initiatives identified in the transition strategy and specific investments in the agency's investment portfolio. In accordance with guidance provided in OMB Circular A-11, agency investments should be matched to the appropriate segment architectures described in the transition plan. The target segment architecture and transition plan support the creation of a project funding strategy, and the creation of business cases for investments required to implement the target segment architecture. (This should be done prior to submitting the agency's budget to the OMB.)

2.4 Inventory Consistency

Agencies should work towards ensuring consistency in their CPIC, FISMA and EA inventories. The "CPIC inventory" is the agency's IT Investment Portfolio that provides budget estimates for all of the agency's IT spending. This portfolio is reported to OMB each September through the agency's Exhibit 53.

In addition to the CPIC inventory, all agencies should have an inventory of FISMA-reportable systems and applications. As all IT spending must be reported in the agency's IT Investment Portfolio, every FISMA-reportable system and application should align to at least one IT investment reported in the Exhibit 53. It should be noted that this is not necessarily a one-to-one mapping. In many situations, an agency's FISMA inventory will contain more systems and applications than there are IT investments listed in the CPIC inventory. This often occurs as there may be multiple systems/applications reported in one IT investment, such as General Support Systems that are reported in a Consolidated Infrastructure investment.

The EA helps the agency respond to changing business needs, and ensures that potential solutions support the agency's targeted state. The CPIC process helps select, control, and evaluate investments that conform with the EA. The EA informs the CPIC process by defining the technologies and information critical to operating an agency's business, and by creating a roadmap which enables the agency to transition from its current state to its targeted state. A proposed IT solution that does not comply with the EA should not be considered as a possible investment, and should not enter the CPIC process.

The CPIC, FISMA and EA inventories are closely related. Only investments that conform with the agency's EA should be considered for funding. Once selected, the investment is reported in the agency's CPIC inventory and should be included in the agency's target EA. All FISMA-reportable systems and applications should be identified in the agency's EA and they should align to at least one investment in the CPIC inventory.

2.5 Timelines

It is crucial to have an understanding of the timelines associated with capital plans and the budget cycle. Even though the Exhibit 53 and Exhibit 300s are submitted to OMB each September, the budgeting process is not confined to the late summer months. Planning, acquiring, and executing IT security budgets are year-round activities. Figure 2-2 indicates prior year, current year, budget year, and second budget year activities that occur in parallel processes.

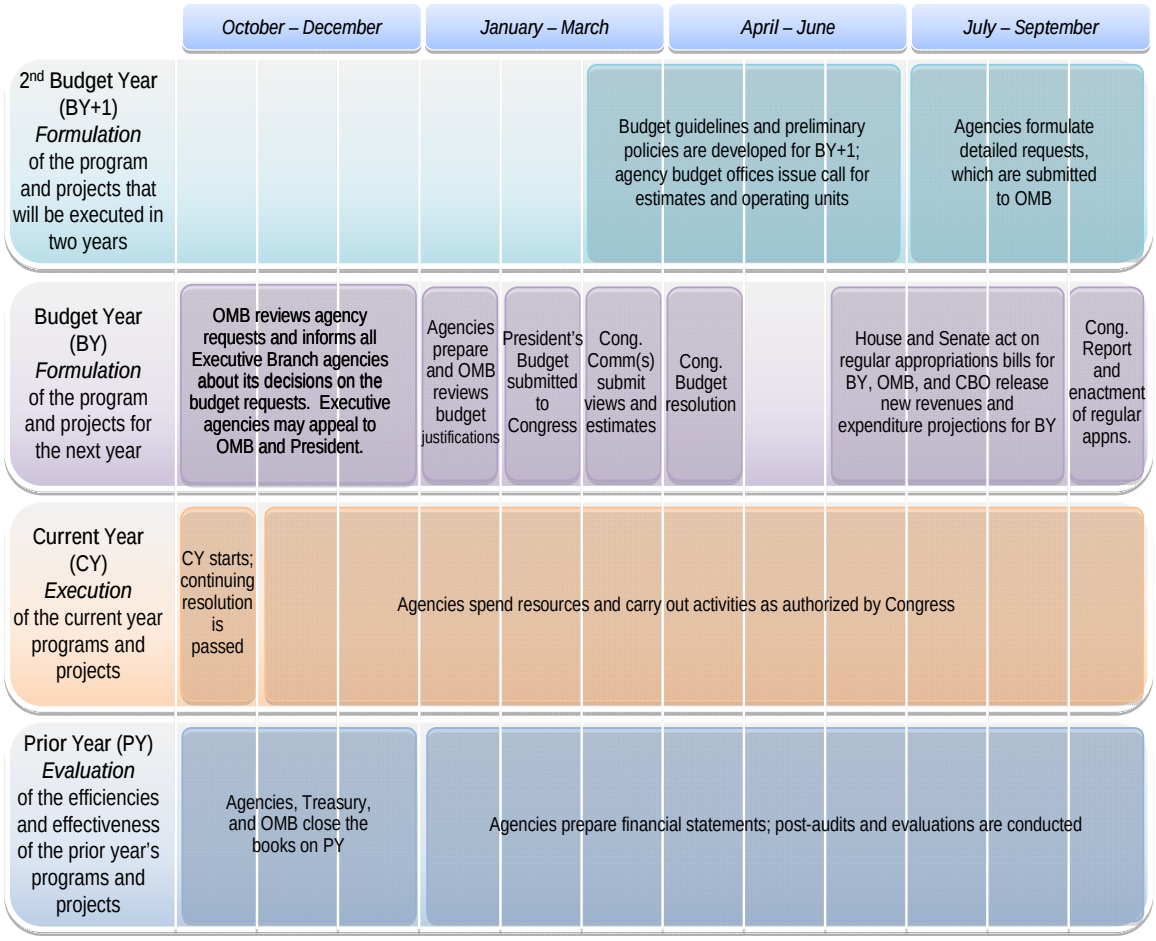

Figure 2-2. Budget Timelines

During the current year, agencies execute their budgets allocated by OMB and Congress. At the same time, agencies evaluate prior year financial and operational performance through audits and evolutions; plan for the next budget year; and begin considering strategies for the second budget year (BY+1).

Figure 2-3 presents the CPIC process point of view for the IT security budgeting timelines. As illustrated in Figure 2-3, with multiple events of the budget process occurring within each Financial Year, it is imperative that agencies use disciplined CPIC processes and controls to streamline activities.

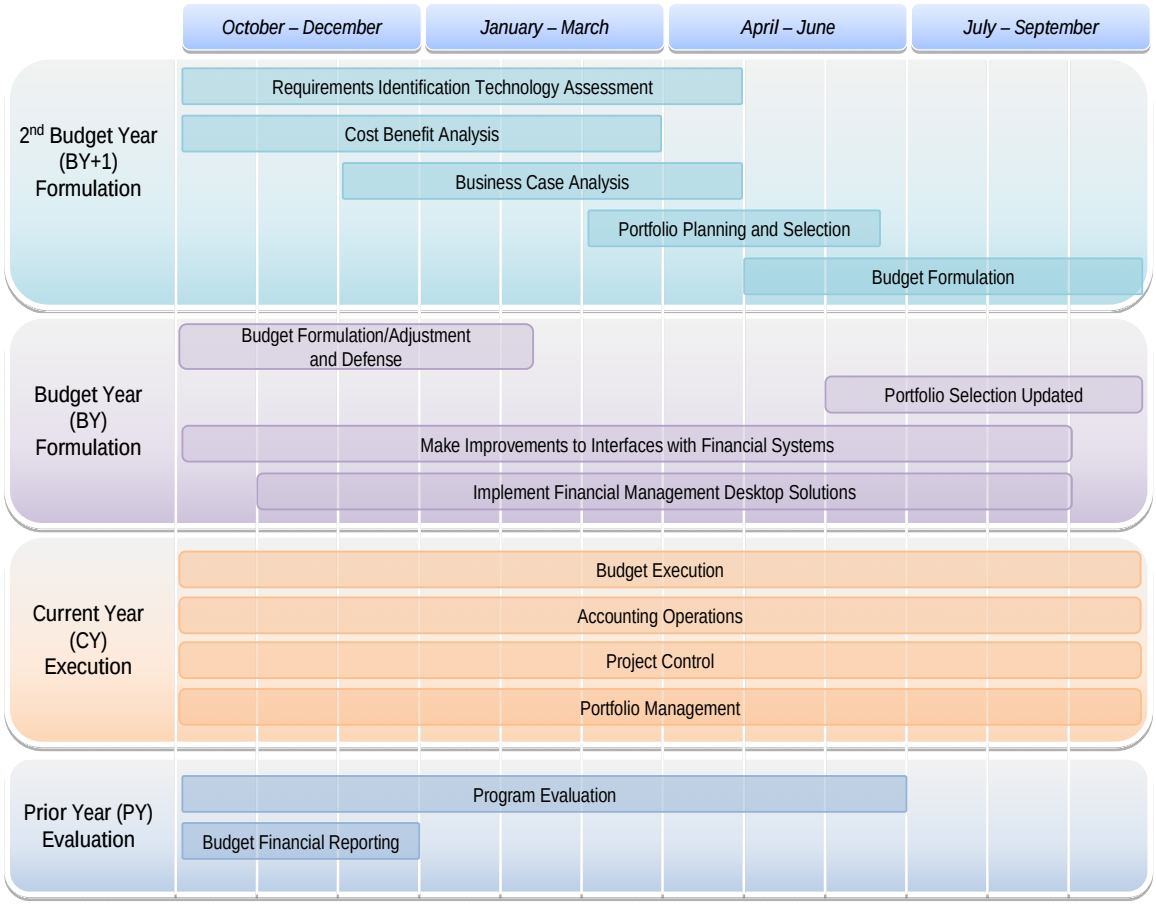

Figure 2-3. CPIC Timelines

Select phase activities performed in the current year are applied to the first and second budget years. During the current year, agencies plan ahead for the two future out-years by identifying potential investments, conducting cost/benefit analyses, developing budgets, and selecting investments to include in the IT investment portfolio.

Control phase activities are performed during the current year as agencies execute their budgets and implement their project controls to ensure schedule and financial milestones are achieved.

Finally, Evaluate phase activities are conducted during the current year for prior year investments to determine whether the investments achieved their intended results.

IT security capital planning is conducted for the future, the present, and the past on a year-round basis. Continual planning, implementation, monitoring, and evaluation leads to a mature CPIC process that not only facilitates improved reporting to OMB and Congress but also leads to an increased security posture and more efficient internal controls and processes.

2.6 Information Security and Capital Planning Integration Roles and Responsibilities

Integrating information security into the capital planning process requires input and collaboration across agencies and functions. Figure 2-4 depicts a hierarchical approach to capital planning in which investment decisions are made at both the enterprise and operating unit levels.

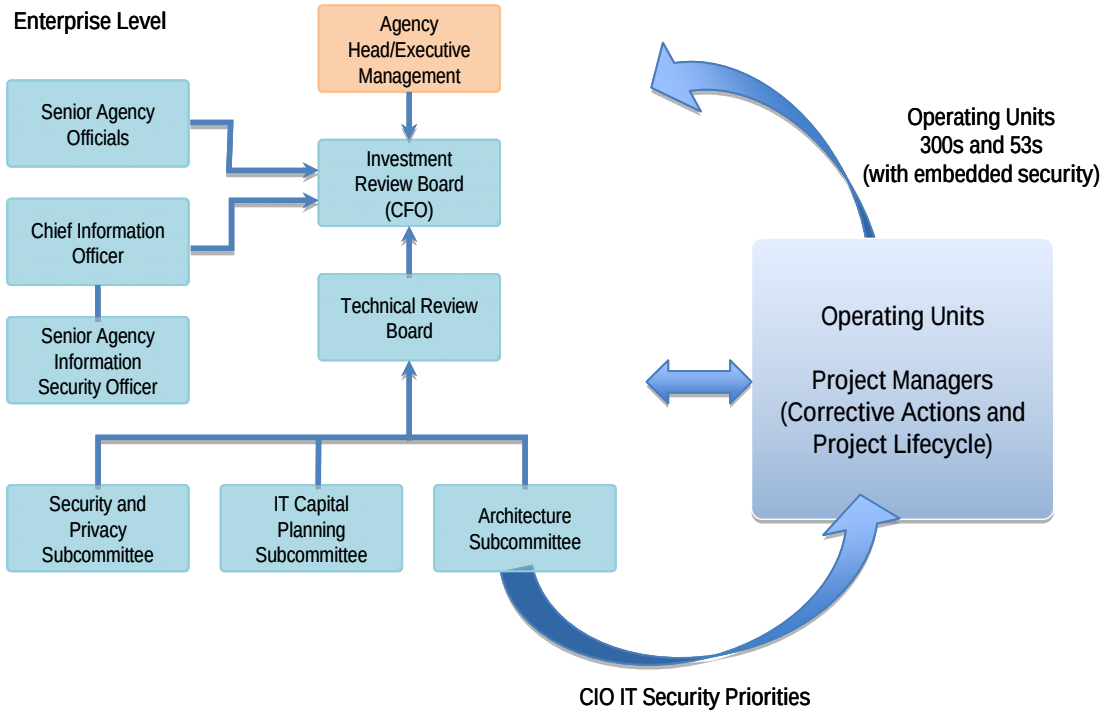

Figure 2-4. Notional IT Management Hierarchy

2.6.1 Investment Management Process

The Chief Information Officer (CIO) formulates and articulates IT security priorities to the organization to be considered within the context of all agency investments. Priorities may be based on agency mission, executive branch guidance and mandates, audits, emerging threats, the importance of specific information and data to the agency's mission, or other external/internal factors. Examples of security priorities include establishing a common continuous monitoring program or implementing PKI throughout the enterprise.

Once operating units finalize their IT portfolios and budget requests for the budget year, they forward their requests to the agency-level decision makers. At the agency level, several committees evaluate IT portfolios from the operating units as referenced in Figure 2-4**,** culminating in a review by the IRB. The IRB then decides on an agency-level IT portfolio and forwards recommendations to the agency head for review. Once the agency-level IT portfolio is approved by the agency head, the necessary Exhibit 300s and Exhibit 53 are forwarded to OMB to obtain funding.

Generally, project managers in operating units manage investments according to federal and agency policies, the CIO-articulated priorities, and specific operating unit priorities. Project managers are also responsible for identifying and documenting vulnerabilities and needed corrective actions for their investments. Each year, project managers prepare and submit Exhibit 300s to the operating unit management and operating unit IRBs. These Exhibit 300s for mixed life-cycle and steady-state investments are combined with Exhibit 300s for new investments and are prioritized at the operating unit level to determine the appropriate IT portfolio mix for the budget year.

The described IT management framework will vary from agency to agency. The important element common to all agencies, though, should be standardized approval hierarchies and parallel planning and prioritization processes at both the enterprise and operating unit levels.

2.6.2 Security and Capital Planning Stakeholders

Many different stakeholders from information security, capital planning, and executive leadership areas play roles in and make decisions on integrating information security into the capital planning process and ultimately forming a well-balanced IT portfolio. Figure 2-5 illustrates the roles and responsibilities hierarchy for integrating information security into the CPIC process. While specific roles and responsibilities will vary from agency to agency, involvement at the enterprise and operating unit levels throughout the process allows agencies to ensure that capital planning and information security goals and objectives are met. Figure 2-5 identifies leading, supporting, or approving roles for each stakeholder as they apply to the integration of security into the CPIC process phases.

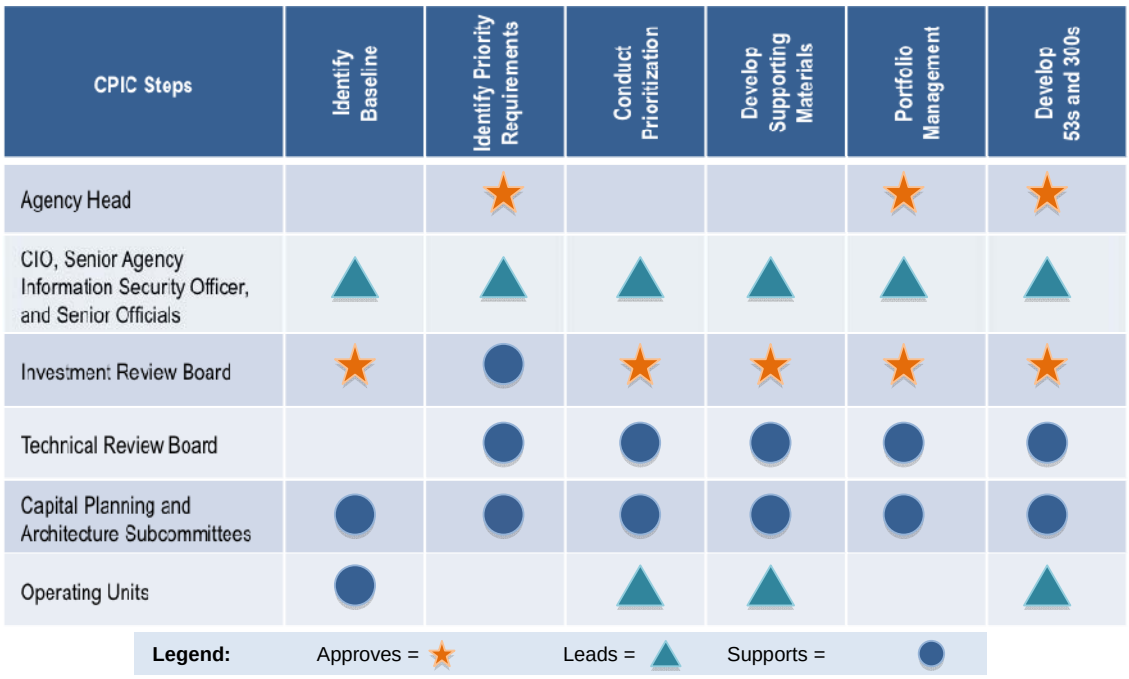

Figure 2-5. Roles and Responsibilities Throughout the CPIC Process

While some roles will vary from agency to agency, sections 2.6.2.1 through 2.6.2.13 describe typical stakeholder roles and responsibilities.

2.6.2.1 Head of Agency

FISMA charges the agency head with ensuring appropriate agency security posture and with reporting to Congress on the status of agency security posture. This position oversees the security policy and the resource budget and has ultimate management responsibility for resource allocation. The agency head has the following responsibilities related to integrating IT security into the CPIC process:

- Complying with FISMA requirements and the related information resource management policies and guidance including OMB Circular A-130 established by the Director of OMB and the related IT standards promulgated by the Secretary of Commerce;
- Ensuring that established information security and resource management policies and guidance are integrated with agency strategic and operational planning processes under FISMA and are communicated promptly and effectively to all relevant agency officials;

- Ensuring that senior agency officials provide information security for the information and information systems that support the operations and assets under their control;
- Establishing strategic agency mission and vision (establishing goals which flow down to budget, IT, and security priorities) and ensuring that information security management processes are seamlessly integrated into those processes and documents;
- Ensuring that the information protection is commensurate with risk and magnitude of harm resulting from the information's compromise;
- Approving the overall annual IT budgets and overall portfolio (with appropriate security integrated) developed through the IRB process;
- Establishing priorities to achieve improvements that comply with the PMA; and,
- Delegating the authority to ensure compliance with agency security requirements to the agency CIO.

2.6.2.2 Senior Agency Officials

Under the direction of the agency head, senior agency officials provide information security for the data and information systems that support the operations and assets under their control. The senior agency official duties include:

- Assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems under their control;
- Determining the levels of information security appropriate to protect information and information systems under their control;
- Implementing policies and procedures to cost-effectively reduce risks to an acceptable level;
- Periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented; and,
- Providing the mission and senior advice to the head of each agency and to the IRB.

2.6.2.3 Chief Information Officer

The Clinger-Cohen Act requires agencies to appoint CIOs. The agency CIO is the senior IT advisor to the IRB and to the head of the agency. In this capacity, the CIO role includes:

- Assisting senior agency officials with IT issues;
- Developing and maintaining an agency-wide information security program;
- Developing and maintaining risk-based information security policies, procedures, and control techniques;
- Designating a Senior Agency Information Security Officer (SAISO) to carry out CIO directives as required by FISMA, including POA&M responsibilities;
- Designing, implementing, and maintaining processes for maximizing the value and managing the risks of IT acquisitions;
- Presenting proposed IT portfolios to the IRB;
- Providing final portfolio endorsements; and,
- Presenting and recommending Control and Evaluate decisions and recommendations.

2.6.2.4 Senior Agency Information Security Officer

The Senior Agency Information Security Officer (SAISO) is appointed by the CIO and manages information security throughout the agency. In some agencies, the SAISO is referred to as the Chief Information Security Officer (CISO) or the Chief Security Officer (CSO). The SAISO is responsible for coordinating program requirements throughout the agency with designated points of contact and project managers. The SAISO's duties include:

- Developing and maintaining an agency-wide information security program;
- Issuing annual information security planning guidance, including security priorities, objectives, and prioritization criteria for new and legacy systems;
- Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities;
- Developing and maintaining information security policies, procedures, and control techniques; and,
- Assisting senior agency officials concerning their information security-related responsibilities.

2.6.2.5 Chief Financial Officer

As a member of the IRB, the agency CFO is the senior financial advisor to the IRB and the head of the agency. In this capacity, the CFO is responsible for:

- Reviewing the cost goals of each major investment;
- Reporting financial management information to OMB as part of the President's budget;
- Complying with legislative and OMB-defined responsibilities as they relate to IT capital investments;
- Reviewing systems that impact financial management activities; and,
- Forwarding personal investment assessments for review by the entire IRB.

2.6.2.6 Investment Review Board

Composed of the CFO and senior managers at the agency or operating unit level, the members of the IRB evaluate existing and proposed IT investments to determine the appropriate mix of investments that will allow the agency to achieve its goals. In this capacity, IRB duties include:

- Approving the CIO's IT strategic guidance, including security priorities and prioritization criteria; these priorities and criteria need to reflect the evolving security needs;
- Approving the controls and evaluating the IT portfolio with embedded security requirements, objectives, measures, and milestones; and,
- Ensuring alignment agency mission and vision with IT security priorities and criteria.

2.6.2.7 Technical Review Board

The Technical Review Board (TRB) is composed of IT security and architecture managers from the Office of the CIO (OCIO) and other applicable members. The TRB's duties include:

- Conducting detailed IT investment review and security analyses and reviewing business cases for security requirements;
- Balancing IT investment portfolios based on CIO/IRB information security priorities and prioritization criteria; and,

- Acting as a focal point for agency coordination of OCIO strategic planning, architectural standards, and outreach to organizations and bureaus.

2.6.2.8 IT Capital Planning, Architecture, and Security and Privacy Subcommittees

The subcommittees provide subject matter expertise and advice to the OCIO and operating units. In this capacity, the subcommittees are responsible for:

- Translating OMB IT capital planning security guidance into operational and internal process control enhancements; and,
- Supplying process improvements and providing EA support for the TRB.

2.6.2.9 Operating Unit/Bureau Executive Management

As representatives of their respective operating units/bureaus within the IRB, operating unit/bureau executive management focuses on the process for integrating information security and privacy priorities into business cases and the OMB Exhibit 53/300 process.

2.6.2.10 Project Manager

The project manager has overall responsibility for coordinating the management and technical aspects of a system's life cycle. Project manager responsibilities include the following:

- Developing a project management plan that integrates security throughout the life cycle;
- Developing a cost and schedule baseline and completing a project within schedule and budget constraints while meeting the customer's needs;
- Coordinating the development, implementation, and operation and maintenance of a system with appropriate units within an agency;
- Reporting the results of projects to the system owner and other appropriate agency staff; and,
- Presenting, when appropriate, the progress of critical projects to the OCIO, the IRB, and other applicable review entities.

2.6.2.11 System Owner

The system owner handles the day-to-day management of the IT investment. The system owner responsibilities include the following:

- Maintaining active senior-level involvement throughout the development of the system;
- Participating in project review activities and reviewing project deliverables;
- Coordinating activities with senior management;
- Obtaining and managing the budget throughout the project's life cycle against a project manager's delivered, locked baseline;
- Holding review and approval authority to ensure that developed products incorporate security and meet user requirements;
- Ensuring system has an up-to-date security plan, has a contingency plan, and receives full C&A;
- Providing baseline assessment performance measures to evaluate the security of the delivered IT initiative; and,
- Developing and maintaining system-specific POA&Ms.

2.6.2.12 Risk Executive Function

The Risk Executive Function provides senior leadership input and oversight for all risk management and information security activities across the organization (e.g., security categorizations, common security control identification) to help ensure consistent risk acceptance decisions. The Risk Executive Function responsibilities include the following:

- Ensuring individual authorization decisions by authorizing officials consider all factors necessary for mission and business success organization-wide;
- Providing an organization-wide forum to consider all sources of risk (including aggregated risk from individual information systems) to organizational operations and assets, individuals, other organizations, and the Nation;
- Ensuring information security considerations are integrated into enterprise architectures, programming/planning/budgeting cycles, and acquisition/system development life cycles;
- Identifying the overall risk posture based on the aggregated risk from each of the information systems and supporting infrastructures for which the organization is responsible; and,
- Ensuring information security activities are coordinated with appropriate organizational entities.

2.6.2.13 Agency Privacy Officer

The Agency Privacy Officer is responsible for ensuring that the services or system being procured meet existing privacy policies regarding protection, dissemination (information sharing and exchange), and information disclosure. The Agency Privacy Officer responsibilities include:

- Conducting privacy impact assessments for electronic information systems and collections and, in general, make them publicly available;
- Posting privacy policies on agency websites used by the public;
- Translating privacy policies into a standardized machine-readable format;
- Reviewing security and privacy sections of the Exhibit 300s; and,
- Reporting annually to OMB on compliance with section 208 of the E-Government Act of 2002.

3. Integration of Security and the Capital Planning and Investment Control Process

3.1 Integration Overview

Agencies have numerous security considerations competing for funding. Security considerations may be:

- New – e.g., a new system, a new release of an existing system or a new mandate;
- Existing – e.g., maintenance activities such as annually testing security controls or conducting a recertification; or,
- Corrective – e.g., addressing POA&M corrective actions.

Agencies can use criteria and weighting factors to rank security drivers through a risk-based prioritization. Based on the output, agencies can then decide which security considerations should be addressed immediately and funded through the current operating budget; which security considerations should be delayed and seek new funding through the budget request; and which security considerations will not be funded and the residual risk will be accepted. Figure 3-1 illustrates the risk-driven inputs to agency security investment decision making and the subsequent options agencies can pursue to implement desired security investments.

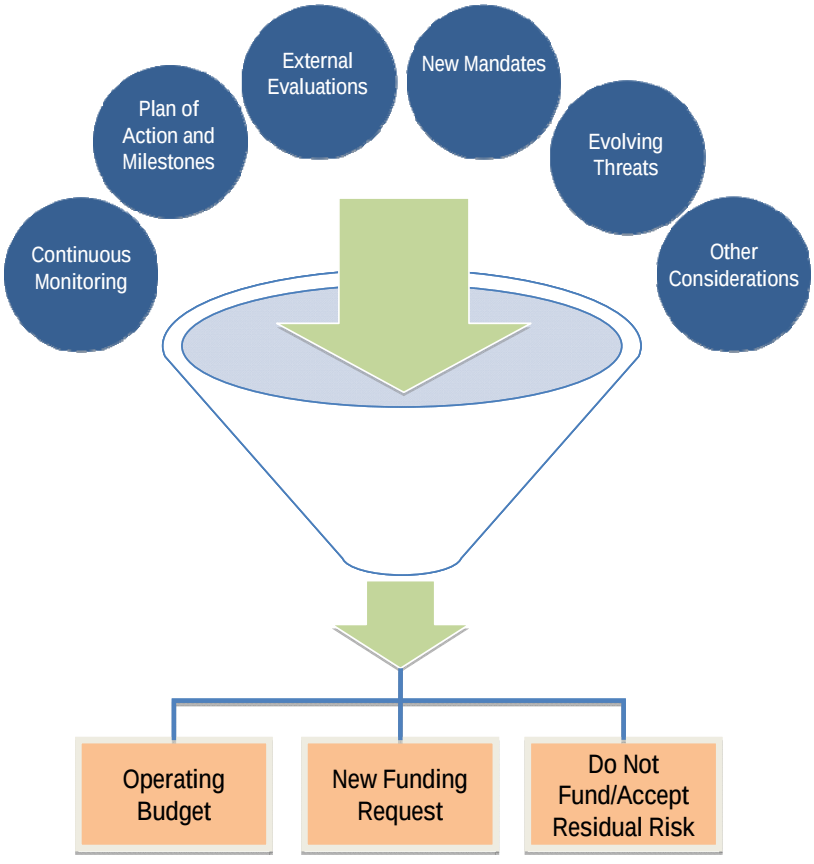

Figure 3-1. Security Investment Decision Making Process

3.2 Decision Making Inputs

While specific inputs will vary slightly from organization to organization, Figure 3-1 illustrates typical inputs to agency information security investment decision making, including:

- Continuous monitoring results;
- Vulnerabilities and associated corrective actions/remediation activities logged into POA&Ms;
- Vulnerabilities and associated corrective actions/remediation activities identified in external evaluations (e.g., General Accountability Office [GAO] and Inspector General [IG] audits and analyses);
- New mandates (e.g., OMB mandates, which are often unfunded);
- Evolving threats, such as zero-day exploits, incidents, warnings and bulletins from United States Computer Emergency Readiness Team (US-CERT), and other associated threats; and,
- Other considerations, including organization-specific activities.

The following sections will address each of these topics in greater detail.

3.2.1 Continuous Monitoring

Continuous monitoring should form the basis of an agency's information security program.[13] While traditional annual security reviews and audits are useful for conducting assessments of system security controls, periodic reviews are limited by their static nature—they cannot account for the evolving threat landscape facing most information systems. As such, truly effective risk-based information security programs should also include a continuous monitoring program integrated with SDLC processes to check the status of subsets of the security controls in an information system on an ongoing basis.

Continuous monitoring programs allow organizations to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the system (including hardware, software, or firmware changes), the environment in which the system operates, and the threats facing the system. A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information to appropriate organizational officials in order to take appropriate risk mitigation actions and make credible, risk-based decisions regarding the operation of the information system. Continuous monitoring programs provide organizations with an effective mechanism to update security plans, security assessment reports, and plans of action and milestones.

The criteria for selecting which security controls to monitor and for determining the frequency of such monitoring should be established by the information system owner or common control provider in collaboration with the authorizing official or designated representative, CIO, senior agency information security officer, and risk executive function. The criteria should reflect the organization's priorities and importance of the information system (or in the case of common controls, the information systems inheriting the controls) to organizational operations and assets, individuals, other organizations, and the Nation in accordance with FIPS 199. Organizations should use recent risk assessments, results of previous security assessments, and operational requirements in guiding the selection of security controls to be monitored and the frequency of the monitoring process.

[13] NIST SP 800-39 Rev. 1, *Guide for Security Authorization of Federal Information Systems: A Security Life Cycle Approach,* provides an overview of continuous monitoring.

The results of continuous monitoring should be reported to the authorizing officials and senior agency information security officers on a regular basis. With the use of automated support tools and effective organization-wide security program management practices, authorizing officials should be able to access the most recent documentation in the authorization package at any time to determine the current security state of the information system, to help manage risk, and to provide essential information for reauthorization and capital planning decisions.

3.2.2 Plan of Action and Milestones

POA&M assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. Throughout the investment life cycle, the POA&M is used to identify security weaknesses and track mitigation efforts for agency IT investments until the weakness has been successfully mitigated. OMB requires agencies to prepare and submit POA&Ms for all programs and systems where an information security weakness has been found. A weakness can be thought of as the gap between current program and system security status and the intended goal/requirement. For example, operating without a contingency plan is a weakness if the system is supposed to have a contingency plan. The POA&M in this example would detail the tasks, resources, and milestones necessary to develop, implement, and test a contingency plan. The resources in this example would need to be funded, which is why the POA&M is a key input to capital planning considerations.

Many times, similar weaknesses appear across multiple system-level POA&Ms. On such occasions, agencies can achieve economies of scale by elevating the system-level weakness to an enterprise-level weakness and developing an associated funding strategy for a new investment to mitigate the weakness at the enterprise-level. For example, if multiple systems are operating without a contingency plan, this weakness can be addressed at an enterprise level by adopting an agency-wide contingency plan template that can be tailored to each system's needs . In addition, key personnel could be identified to develop the contingency plans as well as other continuity operations planning requirements. Because the POA&M can be used to track weaknesses at both the agency and system/program level, and it contains the costs/resources necessary to mitigate the identified weaknesses, it is valuable to the capital planning methodology presented in this guidance.

Prior year (PY) FISMA reporting guidance codifies the exact reporting requirements of the POA&M and should be referenced to ensure the agency is reporting required information to OMB. Table 3-1 contains ten reporting sections that are typically found in POA&M reporting guidance. However, as previously stated, agencies should reference PY FISMA reporting guidance to ensure they report desired information to OMB. In addition to the POA&M sections listed in Table 3-1, all POA&Ms must contain a unique project identifier. This identifier, which appears in the POA&M, the Exhibit 300, and the Exhibit 53, ties the security costs for the corrective actions in the POA&M to the annual budget information contained in the Exhibit 300 and the Exhibit 53.

POA&M Section	Content
Weakness I.D.	Provides a unique project identifier or weakness number for each weakness for tracking purposes.
Weakness	Refers to a specific identified program or system weakness.
Point of Contact	Identifies the office or organization held accountable for correcting weakness.
Resources Required	Details the funding and/or personnel necessary to mitigate the weakness.
Scheduled Completion Date	Indicates corrective action completion date.
Milestones with Completion Dates	Refers to major that occur while completing the corrective action. Timelines and dates are required for each step.
Changes to Milestones	Indicates any changes to timelines.
Source	Identifies how/where the weakness was identified (e.g., risk assessment).

POA&M Section	Content
Status	Indicates if a corrective action is ongoing, delayed, or completed.
Comments	Provides additional detail or clarification (e.g., causes for delays or potential factors that will impact weakness mitigation

Table 3-1. POA&M Reporting Sections[14]

3.2.3 External Evaluations

The results of external security evaluations by entities such as agency GAO and IG can unveil security weaknesses and vulnerabilities that require remediation. Often these remediation activities require funding outside of agencies' pre-planned budgets. In such instances, agencies will have to balance need versus funding considerations to effectively plan and meet the requirements levied upon them by such evaluations.

Agency GAO and IG reports may include recommendations and a specific timeline to implement these recommendations. Agencies should work with the GAO and IG to ensure that these recommendations can be implemented within the required time frame. Within the GAO framework, agencies can reply directly to the GAO through the agency two responses to the report. Once the required timeframe is established, agencies should follow the decision making process to decide how to fund the recommendations.

3.2.4 New Mandates

New laws and/or regulations may impose security mandates on agencies. There are several categories of mandates, including: Presidential Decision Directives, Executive Orders, OMB memoranda, and new public laws. Presidential Decision Directives, such as National Security Presidential Directives and Homeland Security Presidential Directives, outline the policies of the President. If the new policy requires action by the federal departments and agencies a completion date is included within the directive. Through executive orders, the President manages the operations of the federal government and may require departments and agencies to change operations and/or procedures. New public laws are enacted by Congress and set out new regulations and requirements that may or may not be funded. Finally, OMB memoranda often provide guidance and timelines for new policy implemented throughout the federal government.

If new security mandates are not supported by existing funding, departments and agencies should make informed judgments regarding the application of limited resources.

3.2.5 Evolving Threats

Even though agencies actively monitor their security postures through continuous monitoring, inevitably, new vulnerabilities, warnings, incidents, and threats will require agencies to take immediate action to address specific weaknesses and vulnerabilities. Much of the information regarding evolving threats such as incidents and warnings is passed to the federal government through US-CERT federal information notices. Often times these notifications require departments and agencies to use resources to take action and implement changes to mitigate risk and further secure the networks. Such threats often require immediate action using existing or redirected funds. Organizations should make informed judgments regarding the application of limited resources when responding to evolving threats.

[14] OMB Memorandum M-02-01: Memorandum for the Heads of Executive Departments and Agencies

3.2.6 Other Considerations

Specific considerations for identifying security requirements will differ at each agency due to varying missions, strategic goals, and objectives. The phase of the investment in the Select, Control, and Evaluate model will also impact the inputs. For example, investments in the Select phase represent proposed initiatives. Requirements may be identified based on the security controls needed to address the sensitivity, criticality, and value of the investment. During the Control phase, investments progress from development to implementation. The investment's security performance is monitored and corrective actions are identified as necessary. Investments in the Evaluate phase are fully deployed and undergo periodic reviews to assure that they are producing the benefits expected, are adhering to enterprise EA and security requirements, and meeting the agency's evolving mission goals and priorities. Adjustments should be made where appropriate.

3.3 Investment Decision Making

Once security considerations have been identified, agencies must determine which considerations should be implemented. Funding and resources are not always available to cover all security needs, therefore considerations must be prioritized to address the most pressing security needs first and to ensure the most effective use of resources. To effectively prioritize security considerations, agencies must identify criteria for prioritization. Specific prioritization criteria will vary from agency to agency; however, a common approach is to rank order information security considerations. Agency management and stakeholders should be involved in the process of identifying the prioritization criteria.

3.3.1 Prioritization Scheme

A prioritization scheme may be used to rank order security considerations and to determine which needs should be funded.[15] The process involves identifying the criteria that will be used to assess each security consideration. Next, each criterion is assigned a weight according to the priorities of the organization. Each security consideration is then assessed to determine how well it meets the intent of each criterion. Finally, a "score" may be assigned to each security consideration, which may be used to rank-order needs and identify those that should be funded.

3.3.2 Prioritization Stakeholders

Multiple stakeholders should collaboratively work to determine the prioritization criteria and its weights, as well as validate the assessment . Stakeholders may include the CIO, senior security officials, key system owners, and members of the IRB. The stakeholders involved in each of these activities will vary from agency to agency depending upon the size, maturity, and mission of the agency. It is important to involve stakeholders with the authority to make decisions. It is also important that the stakeholders include both security practitioners and individuals familiar with capital planning requirements. In addition, stakeholders with the authority to make decisions should be included in the process. Senior decision makers provide a positive impact because they possess insight on the security posture, EA, and budget requirements/constraints across the operating unit/enterprise; have the authority to approve funding; and are accountable for enacting change.

A high degree of coordination is required to perform these activities successfully to ensure buy-in from all parties. It is important to bring stakeholders together early in the process and involve them throughout the process. It also may be helpful to have a facilitated session using a decision support tool to coordinate input from multiple parties.

[15] Note – the prioritization scheme presented in this guidance is meant to serve as an example only. Agencies should use prioritization approaches that are tailored to their unique environments.

3.3.3 Prioritization Criteria and Weights

Each agency should develop their prioritization criteria and its weights based on agency mission and goals. The criteria and weights may change and evolve overtime. Examples of general prioritization criteria include:

- Threat/Impact – what is the potential impact if the remediation or security investment is not addressed?
- Likelihood – is the consequence that could result from not addressing the remediation or security investment something that is likely to manifest?
- Cost - roughly, how much will the remediation or security investment cost the agency?
- Cost-effectiveness – will the remediation or security investment address multiple security requirements?
- Feasibility – is the recommended remediation or security investment technically and/or operationally feasible?
- Agency's Mission – how important is the remediation or security investment to the agency's mission and goals?

3.3.4 Assessment and Ranking

Once agency management and stakeholders agree on prioritization requirements, the agency must begin the ranking process by assessing the security considerations against the prioritization criteria. Each security consideration is assigned a quantitative value that represents the consideration's ability to meet the intent of the criterion. Once all security considerations have received an assessment for each criterion, the assessment value is multiplied against the criterion weight. All weighted values are then added together to obtain a total score for the security consideration. The total scores may then be compared to rank-order the security considerations.

Security considerations with the highest score represent the top priority or most critical security investments. The objective is to apply the first security dollar to the most critical security investment. The next dollar is then applied to the next critical security investment and so forth until the security budget is expended.

3.3.5 Prioritization Scheme Example

The following example provides an illustration of how the prioritization scheme explained in Sections 3.3.1 – 3.3.4 may be applied.[16] The example assumes the prioritization criteria will be those listed in Section 3.3.3.

Once the prioritization criteria have been identified, the next step is to assign a weight to each criterion. Weights may be a percentage in which the total weight for each criterion adds up to 100%; or criteria may be assigned a Low/Moderate/High weight which corresponds to 1, 2, 3 respectively. The key is to ensure that all weights represent a realistic quantitative value. Table 3-2 provides an example of using both the percentage and Low/Medium/High weighting. In this example, the agency has placed a strong priority on Threat/Impact, Cost-Effectiveness, Feasibility and Agency's Mission. The agency has placed the lowest priority on Likelihood.

[16] The examples are merely illustrative and are not compulsory.

Criteria	Percentage Weight	Low/Moderate/High Weight
Threat/Impact	20%	High (3)
Likelihood	5%	Low (1)
Cost	15%	Medium (2)
Cost-Effectiveness	20%	High (3)
Feasibility	20%	High (3)
Agency's Mission	20%	High (3)

Table 3-2. Notional Investment Weighting Criteria

After assigning the weight to each criterion, each security initiative being considered for funding is assessed against the criteria to determine how well it meets the intent of the criteria. This may be done by assigning a quantitative value. Any scale may be used, such as a value of 1 to 10, in which "10" indicates that the security consideration fully meets the intent of the criterion; or a Low/Moderate/High, corresponding to a 1, 2, 3 may be used. The key is to ensure a consistent scale is used across all considerations.

Table 3-3 provides an example of using both the 1-10 scale and the Low/Medium/High assessment. In the example, three security initiatives are being considered for funding. Each initiative has been assigned a value "score" for each criterion. Each score is based on the stakeholders' assessment of how well the initiative meets the intent of the criterion.

Criteria	Security Requirement #1		Security Requirement #2		Security Requirement #3	
Threat/Impact	9	High (3)	2	Low (1)	4	Medium (2)
Likelihood	3	Low (1)	8	High (3)	6	Medium (2)
Cost	5	Medium (2)	7	High (3)	9	High (3)
Cost-Effectiveness	8	High (3)	2	Low (1)	3	Low (1)
Feasibility	9	High (3)	3	Low (1)	8	High (3)
Agency's Mission	6	Medium (2)	4	Medium (2)	7	High (3)

Table 3-3. Notional Requirement Assessment

- Threat/Impact – The stronger the potential impact of the threat being exploited, the higher the assessment value.
- Likelihood – The more significant the likelihood of the threat being exploited, the higher the assessment value.
- Cost – A higher assessment value is assigned to investments with lower costs.
- Cost-effectiveness – A higher assessment value is assigned to investments that will address multiple security requirements.
- Feasibility – A higher assessment value is assigned to more feasible investments.
- Agency's Mission – A higher assessment value is assigned to investments that are important to the agency's mission and goals.

The final step is to calculate a total score for each security consideration. This is accomplished by multiplying the weight of the criterion by the score assigned for the criterion. The weighted score for each criterion is added together to arrive at a total score for the initiative. Table 3-4 and Table 3-5 provide examples of how to calculate a score based on the weights and value scores assigned in Table 3-2 and Table 3-3.

Criteria	Weight	Initiative #1	Initiative #2	Initiative #3
Threat/Impact	20%	20% x 9	20% x 2	20% x 4
Likelihood	5%	5% x 3	5% x 8	5% x 6
Cost	15%	15% x 5	15% x 7	15% x 9
Cost-Effectiveness	20%	20% x 8	20% x 2	20% x 3
Feasibility	20%	20% x 9	20% x 3	20% x 8
Agency's Mission	20%	20% x 6	20% x 4	20% x 7
TOTAL SCORE:		**7.3**	**3.65**	**6.05**

Table 3-4. Requirements Analysis – Percentage-Based

Criteria	Weight	Initiative #1	Initiative #2	Initiative #3
Threat/Impact	High (3)	3 x 3	3 x 1	3 x 2
Likelihood	Low (1)	1 x 1	1 x 3	1 x 2
Cost	Medium (2)	2 x 2	2 x 3	2 x 3
Cost-Effectiveness	High (3)	3 x 3	3 x 1	3 x 1
Feasibility	High (3)	3 x 3	3 x 1	3 x 3
Agency's Mission	High (3)	3 x 2	3 x 2	3 x 3
TOTAL SCORE:		**38**	**24**	**35**

Table 3-5. Requirements Analysis – Low/Medium/High

Once all security initiatives have been assessed and a total value score has been calculated, stakeholders can rank-order the initiatives. Security initiatives with the highest score represent the top priority or most critical security investments. Funding should first be applied to the most critical security investment. Funding is then applied to the next critical security investment and so forth until the available budget is expended.

In the example above, if the agency had to choose between funding the three security initiatives, the priority would be Initiative 1, Initiative 3, and, finally, Initiative 2. Initiatives 1 and 3 are close in value score; however, the higher score for Initiative 1 is due to its perceived ability to address the criteria most important to the agency.

Both Initiatives 1 and 3 are assessed as having a High rating in three of the criteria, a Medium rating in two of the criteria and a Low rating for one criterion. Though criteria ratings are similar, once the ratings are weighted against each criterion's priority, differentiation occurs. Initiative 1 has a high rating in three of the four highest weighted criteria; whereas Initiative 3 has a high rating in only two of the four highest weighted criteria. Also, Initiative 3 has a low rating for one of the highest weighted criterion, while Initiative 1 has either high or medium ratings for all of the highest weighted criteria.

Initiative 2 is rated as having a high likelihood that a security risk will be exploited. This implies the threat is likely to be realized if the security initiative is not implemented. Though the likelihood is high, the impact if the threat is exploited is perceived to be low. Also, the cost to implement Initiative 2 is expensive and the feasibility is low. For these reasons, Initiative 2 received the lowest value score and is the least critical security investment.

3.4 Outputs/Decisions

Armed with the appropriate inputs, stakeholders, and decision criteria, agencies can make informed, risk-based capital planning decisions. Agencies typically decide to take one of three courses of action during the decision making process:

- Immediately fund the security need through the operating budget – this method is primary used for immediate needs; for example, responding to an incident. It involves using the current security budget for the investment or reallocating existing funds and/or personnel.
- New funding request – this method is primarily used to request additional funding through the budget submission to address security concerns. Depending upon the scope of the funding necessary:
    - An increase in funding to an existing investment may be required to remediate a weakness; for example, funding that will be used to address a system-level weakness. The budget year funding request identified in the Exhibit 53 (and if applicable, the Exhibit 300) should include the dollar amount required to remediate the weakness.
    - A new investment may be necessary that will require significant capital; for example, a weakness that is pervasive across several POA&Ms that will require an enterprise-level investment to resolve. This will require a new investment to be approved during the Select phase and the agency's IT portfolio will be updated to include the investment. If the investment is considered a "major" investment, an Exhibit 300 must prepared for the budget submission; if the investment is considered a "non-major," it will be reported in the Exhibit 53 only.
- Do not fund and accept the risk – this option is chosen when the cost of the proposed investment significantly outweighs the likelihood and impact of the threat being exploited.

3.4.1 Existing Funds

Agencies may use their current budget or reallocate existing resources to address a security need. Before spending funds to perform new development, enhancements, or modifications to an information system, an agency should apply that funding to address its pressing security needs. Each agency's budget request should be risk-adjusted to address unknown and/or unexpected costs. Security concerns must be considered when risk-adjusting the life cycle cost for an investment.

All risks contribute to the calculation of risk-adjusted cost. OMB requires the budget request for each IT investment to be risk-adjusted. The risk-adjusted cost calculation provides a range of how the investment's costs will be affected if part or all the investment and security risks identified in the Risk Management Plan manifest themselves. The risk-adjusted costs provide realistic forecasts across the investment life cycle, allowing decision-makers to plan appropriately for risks to the investment.

3.4.2 New Funding

Agencies seeking new funding to address security needs may request the funding through an existing investment in its IT Portfolio or create a new investment.

The funding required to develop, operate, and maintain each FISMA system should be reported in one of the investments included in the agency's IT Portfolio. Agencies may request an increase in system-level funding through the existing Exhibit 300 (for major investments) or Exhibit 53 (for non-major investments). Both the Exhibit 300 and the Exhibit 53 request the percentage of the budget year request that is for information security. The dollar amount identified for security should include the increase being requested. In addition, the Exhibit 300 asks whether an increase in information security funding is requested to remediate information security weaknesses. If the additional funding will be used to address a remediation action, a "yes" response should be provided and both the dollar amount required to remediate the weaknesses and a description of how the funding will be used should be given.

Funding may also be requested for a new initiative, which will address an enterprise-wide security need. This will require the agency to add the investment to the agency's IT Portfolio through the Select process. If the new initiative is a non-major investment, it will be reported in the agency's Exhibit 53 only. If the new initiative is a major investment, a business case and Exhibit 300 will be required. In such cases, the following steps will be necessary:

- Concept Paper: The concept paper is developed by the investment owner and submitted to the IRB for review. The concept paper provides a high-level description of the proposed investment and includes a rough-order-of-magnitude costing estimate, benefits, milestones and agency impacts. Such papers are usually only a few pages long. Based on the concept paper, the IRB can determine whether the investment will be a worthwhile endeavor and recommend continuation or cancellation of the potential investment.

- Business Case: Following approval of a concept paper, the next step is to develop a business case analysis (BCA) for IRB review. The BCA process is important in the selection of an investment because it enables decision-makers to consider the potential of several investment alternatives before making an acquisition decision. The objective of a BCA is to measure and illustrate the full impact of an investment within distinct functional areas to make cost and benefit projections on a larger scale. The result of the BCA is clearly the justified selection of a preferred alternative for investment consideration. The BCA provides a consistent framework for looking at key variables such as cost of the alternative, benefits the alternative yields, and associated investment risk. These factors can then be compared across a range of alternatives so a single investment alternative can be selected. A well-prepared BCA incorporates both financial metrics and non-financial factors into a concise and informative presentation. The BCA should also clearly address key issues and facts while revealing the investment's contribution in context to the entire agency and its mission. The following objectives are the components necessary to compose a comprehensive BCA:

    - Evaluate Mission and Objectives. The BCA should identify the agency's mission and objectives and explain how the investment will enable the agency to fulfill them.

    - Assess Current Environment. The status quo environment or the way processes are performed today, should be thoroughly explained in the context of the agency's "to-be" EA blueprint.

    - Perform Gap Analysis. The BCA should include a discussion of the desired "to be" state. In other words, it should describe the optimal environment to support the agency mission and goals, and point out the necessary steps, procedures, etc., that lie between the status quo and the optimal environment.

    - Identify Investment Alternatives. The BCA should identify investment alternatives in accordance to budget year Exhibit 300 guidance to reach the optimal environment described in the Gap Analysis.

- Estimate Cost. A defined cost element structure should be included for each alternative, and life-cycle costs should be incorporated to demonstrate the financial impact of each alternative across the investment life cycle.

- Perform Sensitivity Analysis. Individual cost assumptions and variable values should be adjusted over specified ranges, and the total costs should be estimated. The resulting relationship between changes in total cost and changes in each variable can be quantified to capture the sensitivity of each variable/cost.

- Characterize Benefits. Benefits that will accrue as a result of each alternative should be identified and quantified where possible. When quantifiable, the benefits should be compared against life-cycle cost estimates to demonstrate any possible returns on the investment.

- Perform Risk Analysis. Investment risk analyses (including security risks) should be conducted for the alternatives, and costs should be adjusted commensurate with anticipated risk.

Once business cases are approved by the agency IRB, the agency must summarize the results of the BCA in the Exhibit 300. The Exhibit 300 is submitted to OMB in early September with the agency's budget request. Exhibit 300s are discussed on more detail in section 3.5.4. Additionally, Appendix D. Exhibit 300 Guide to Security Section provides a detailed overview of specific security requirements in the Exhibit 300.

3.4.3 Accept Residual Risk and Do Not Fund

Agencies may choose to accept the risk and not fund new security investments or specific remediation actions. This approach should be taken if the cost of the proposed investment significantly outweighs the likelihood and impact of the threat being exploited. This approach may also be chosen if it is determined that the security investment or specific remediation action is technically and/or operationally infeasible.

3.5 Implementation

After approving new funding for investments or redirecting funding in response to specific requests, agencies should implement and monitor these investments.

3.5.4 Exhibit 300 Overview

To submit a funding request for a major IT investment, agencies must use the Exhibit 300 (which is also called the OMB Capital Asset Plan). The Exhibit 300 documents the business case for making a major IT investment. It is designed to coordinate OMB's collection of agency information for its reports to Congress; ensure that the business cases for IT investments are made and tied to the mission statements, long-term goals and objectives, and annual performance plans; ensure that security, privacy, records management, and electronic transactions policies are fully implemented for IT; and help identify poorly performing projects. It is the document that OMB uses to assess investments and ultimately make funding decisions.

The Exhibit 300 documents all of the planning and management activities associated with a particular IT investment throughout the investment lifecycle, from initial concept to termination/replacement. It represents a commitment on the agency's part to manage the investment exactly as is documented in the Exhibit 300 and to meet the cost and performance goals outlined in the document.

OMB evaluates each Exhibit 300 based on ten criteria:

- President's Management Agenda;

- Project Management;
- Acquisition Strategy;
- Performance Information;
- Security;[17]
- Privacy;
- Enterprise Architecture;
- Alternatives Analysis;
- Risk Management; and,
- Cost/Schedule/Performance.

Investments receive a score of 1-5 for each criterion, with "5" representing the best score. In order to "pass," the Exhibit 300 must have a cumulative score of at least 31; receive at least a "4" in Security; and receive at least a "3" for all other criteria. Any investment not meeting all three requirements is placed on OMB's Management Watch List.

Investments are placed on OMB's Management Watch List as a result of not meeting standards. If an investment's Capital Asset Plan contains one or more weakness, it is placed on OMB's Management Watch List and targeted for follow-up action to correct possible problems. The Management Watch List is one tool used by OMB to monitor agency planning and drive improved portfolio management.

The Management Watch List is not to be confused with the High Risk List. OMB's High Risk List contains a set of high-priority IT projects. The projects on the list are not necessarily experiencing management problems or are in danger of failing. Instead, they are placed on the list because they are considered high-profile IT investments that require special attention from the agency's senior managers. Reasons a project may require special attention include its complexity, high cost, or its level of importance.

Appendix D. Exhibit 300 Guide to Security Section, contains additional information on the security requirements within the Exhibit 300.

3.5.5 Continuous Monitoring and Assessment

Once agencies submit Exhibit 300s to OMB, and receive and allocate funding to investments and programs to investment in new security investments or to remediate specific vulnerabilities in existing investments, agencies must maintain vigilant continuous monitoring and assessment programs. As discussed in Section 3.2.1, continuous monitoring helps ensure that remediation activities are mitigating risk as anticipated and that new weaknesses do not manifest. Continuous monitoring and assessment throughout the investment lifecycle help ensure that as the operating environment changes, the investment's security controls and security posture are positioned to adequately protect the investment. In cases where continuous monitoring results indicate that additional mitigation activities are warranted, they can be planned for through the CPIC process.

3.6 Other Issues

Despite thorough security planning, implementation, and continuous monitoring activities, obtaining "perfect" security is an elusive goal given rapidly changing technologies and the growing sophistication

[17] See Appendix D. Exhibit 300 Guide to Security Section for specific guidance on Exhibit 300 security considerations.

of threat actors. Not only is perfect security virtually unobtainable, the cost to try to achieve it is prohibitive and not easily justifiable. When funding information security, agencies must consider both the technical and economical feasibility of the investment. Agencies should strive for a risk-based balance between threats, consequences, and costs to mitigate vulnerabilities and reduce risk through effective security control and security program implementation.

Even with the best security controls in place, systems can be compromised. The reality is that cyber attacks have the potential to exploit federal networks. When a compromise occurs, agencies must be able to restore and recover their networks while maintaining an operational state. A lot of attention and dollars are focused on prevention mechanisms; however, simply securing a system or network is not sufficient. A comprehensive security program must also include detection and recovery components to facilitate operations under stress.

Information security is a dynamic process that must be effectively managed. Once agencies have identified and implemented baseline security controls, they must assess the effectiveness of these controls and make adjustments where necessary. In managing evolving threats, changes in a system's environments and limited resources, agencies must revaluate their priorities and assign resources to the most critical issues.

Appendix A. Glossary[18]

- **Capital planning and investment control (CPIC)** – a synonym for capital programming and is a decision-making process for ensuring that information technology (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.
- **The Clinger-Cohen Act of 1996** – legislation that requires agencies to use a disciplined CPIC process to acquire, use, maintain and dispose of information technology.
- **Federal Enterprise Architecture (FEA)** – a framework that describes the relationship between business functions and the technologies and information that support them. Major IT investments will be aligned against each reference model within the FEA framework.
- **The Federal Information Security Management Act (FISMA) –** requires agencies to integrate IT security into their capital planning and enterprise architecture processes at the agency, conduct annual IT security reviews of all programs and systems, and report the results of those reviews to the Office of Management and Budget (OMB).
- **IT security investment** – an IT application or system that is solely devoted to security. For instance, intrusion detection systems (IDS) and public key infrastructure (PKI) are examples of IT security investments.
- **Life-cycle costs** – the overall estimated cost, both Government and contractor, for a particular program alternative over the time period corresponding to the life of the program, including direct and indirect initial costs plus any periodic or continuing costs of operation and maintenance.
- **Major IT investment** – a system or investment that requires special management attention because of its importance to an agency's mission; was a major investment in the previous budget submission and is continuing; is for financial management and spends more than $500,000; is directly tied to the top two layers of the FEA (Services to Citizens and Mode of Delivery); is an integral part of the agency's modernization blueprint (enterprise architecture); has significant program or policy implications; has high executive visibility; and is defined as major by the agency's CPIC process. OMB may work with the agency to declare other investments as major investments. All major investments must be reported on exhibit 53. All major investments must submit a "Capital Asset Plan and Business Case," Exhibit 300. Investments that are e-Government in nature or use e-business technologies must be identified as major investments regardless of the costs. If unsure about what investments to consider as "major," consult your agency budget officer or OMB representative. Systems not considered "major" are "non-major."
- **Privacy impact assessment** – a process for examining the risks and ramifications of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting information in identifiable form. Consistent with September 26, 2003, OMB guidance (M-03-22) implementing the privacy provisions of the e-Government Act, agencies must conduct privacy impact assessments for all new or significantly altered IT investments administering information in identifiable form collected from or about members of the public. Agencies may choose whether to conduct privacy impact assessments for IT investments administering information in identifiable form collected from or about agency employees.
- **Risk**

[18] Glossary definitions are adapted from OMB Circular A-11, Part 7, Planning, Budgeting, Acquisition, and Management of Capital Assets, and from applicable NIST guidance.

- **Security risk** – the level of impact on agency operations (including mission functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
- **Investment risk** – risks associated with the potential inability to achieve overall program objectives within defined cost, schedule, and technical constraints.

- **Select-Control-Evaluate IT investment management process**
  - **Select –** the goal of the Select phase is to assess and prioritize current and proposed IT projects and then create a portfolio of IT projects. In doing so, this phase helps to ensure that the organization (1) selects those IT projects that will best support mission needs and (2) identifies and analyzes a project's risks and returns before spending a significant amount of project funds. A critical element of this phase is that a group of senior executives makes project selection and prioritization decisions based on a consistent set of decision criteria that compares costs, benefits, risks, and potential returns of the various IT projects.
  - **Control –** the Control phase consists of managing investments while monitoring for results. Once the IT projects have been selected, senior executives periodically assess the progress of the projects against their projected cost, scheduled milestones, and expected mission benefits.
  - **Evaluate** – the Evaluate phase provides a mechanism for constantly improving the organization's IT investment process. The goal of this phase is to measure, analyze, and record results based on the data collected throughout each phase. Senior executives assess the degree to which each project has met its planned cost and schedule goals and has fulfilled its projected contribution to the organization's mission. The primary tool in this phase is the post-implementation review (PIR), which should be conducted once a project has been completed. PIRs help senior managers assess whether a project's proposed benefits were achieved and also help to refine the IT selection criteria to be used in the future.
- **Security controls –** the management, operational, and technical controls (*e.g.*, safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

4. Appendix B. References

Clinger-Cohen Act , 40 United States Code (U.S.C.) 1401 and following, 1996.

Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. Chapter 35, Subchapter III, 2002.

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, November 2000.

OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*, June 2008.

NIST SP 800-37, Rev. 1, Draft *Guide for Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, August 2008.

NIST SP 800-39, Draft *Managing Risk from Information Systems: An Organizational Perspective*, April 2008.

NIST SP 800-53, Rev. 3, Draft *Recommended Security Controls for Federal Information Systems*, February 2009.

NIST SP 800-55, Rev. 1, *Performance Measurement Guide for Information*, July 2008.

NIST SP 800-64, Rev. 2, *Security Considerations in the System Development Life Cycle*, October 2008.

Appendix C. Legislation, Regulation, and Guidance

Title	Requirement
OMB Memoranda	
OMB M-08-16 TIC Statement of Capability Form	Submit the Trusted Internet Connection (TIC) Statement of Capability (SOC) Form to propose a solution and provide a level of capability to become a Trusted Internet Connection Access Provider (TICAP).
OMB M-08-05 TIC	Develop a comprehensive POA&M for TICs.
OMB M-08-09 New FISMA Privacy Reporting Requirements for FY 2008[19]	As part of the FY08 FISMA reports, OMB will require agencies to submit the following information (by agency): • Report the number of each type of privacy review conducted during the last fiscal year; • Report information about the advice provided by the Senior Agency Official for Privacy during the last fiscal year; • Report the number of written complaints for each type of privacy issue allegation received by the Senior Agency Official for Privacy during the last fiscal year; • Report the number of complaints the agency referred to another agency with jurisdiction, for each type of privacy issue received by the Senior Agency Official for Privacy for alleged privacy violations during the last fiscal year.
OMB M-08-01 HSPD-12 Implementation Status	Re-iterates the October 2008 deadline for Personal Identity Verification (PIV) card issuance stated in OMB M-07-06, Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials.
OMB M-07-06 Validating and Monitoring Agency issuance of PIV Credentials	M-07-16 discusses validation and monitoring agency issuance of PIV compliant identity credentials.
OMB M-03-22 OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002	Provides the following guidance on implementing the privacy provisions of the E-Government Act of 2002: 1. E-Government Act Section 208 implementation guidance 2. Section 208 privacy provisions guidance 3. A summary by the Federal Trade Commission (FTC) of its guidance regarding federal agency compliance with the Children's Online Privacy Protection Act (COPPA) 4. A summary of modifications prior to guidance
OMB M-07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information[20]	Variety of updates to OMB M-06-16
OMB M-05-08 Designation of Senior Agency Officials for Privacy	Within 30 days of the issue date of this memo, identify to OMB the senior official who has the overall agency-wide responsibility for information privacy issues. Provide OMB with the name, title, and contact information (phone number and email address) for the senior

[19] Federal Information Security Management Act (FISMA) reporting requirements are announced annually. This memo will be replaced with new requirements for FISMA fiscal year 2009 (FY09) reporting.
[20] Subsumes OMB M-06-16

Title	Requirement
	agency official.
OMB Circulars	
OMB A-11 Preparation, Submission, and Execution of the Budget	Provides guidance on developing agency budget requests.
OMB A-130 Management of Federal Information Resources	Protect government information commensurate with the risk and magnitude of harms that could result from the loss, misuse, or unauthorized access to or modification of such information.
Public Laws	
Federal Information Security Management Act of 2002 (FISMA) (Title III of the E-Gov Act of 2002)	Requires agencies to annually report on the adequacy and effectiveness of information security policies, procedures, and practices.
Electronic Government Act of 2002 (E-Gov)	Provides a means for improving coordination and deployment of IT across the Federal Government, helping agencies achieve the IT management reforms required under the Clinger-Cohen Act, and ensuring greater citizen access to the Federal Government through the improved use of IT.
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Provides protections for citizens who have preexisting medical conditions or might suffer discrimination in health coverage based on a factor that relates to an individual's health. Act has four major objectives: 1) Assure health insurance portability by eliminating job-lock due to pre-existing medical conditions 2) Reduce healthcare fraud and abuse 3) Enforce standards for health information 4) Guarantee security and privacy of health information
Privacy Act of 1974, as amended	Primary law regulating the Federal Government's collection and maintenance of personal information. Directs OMB to develop and prescribe guidelines and regulations. Protects against invasion of privacy caused by misuse of records collected by the Federal Government. Permits individuals to gain access to most personal information maintained by federal agencies and to seek amendment of any inaccurate, incomplete, untimely, or irrelevant information.

Appendix D. Exhibit 300 Guide to Security Section

The following sections provide guidance on how to address the Security section of the OMB Exhibit 300. The guidance is based on OMB Circular A-11, Part 7, Section 300, Planning, Budgeting, Acquisition, and Management of Capital Assets dated June 26, 2008 and OMB's FY2009 Exhibit 300 Evaluation Criteria.

Agencies must incorporate security into their IT investments to ensure that security supports agency business operations and that plans to fund and manage security are built into life cycle budgets for information systems.[21] OMB continues to aggressively address this issue through the budget process. Security is a continuous theme throughout the Exhibit 300 as six of the Exhibit 300 sections have explicit security requirements:

Section	Security Information Required
Summary of Spending Table	All dollars, including security related costs, going toward the investment over its estimated life cycle must be presented in the table
Acquisition / Contract Strategy	Security requirements are addressed in the Acquisition Strategy and all contracts include the required security and privacy clauses
Security and Privacy	Specific security and privacy questions must be addressed at the system/application level
Alternatives Analysis	The life cycle cost estimates for all alternatives include security-related costs and are risk-adjusted
Risk Management	The investment has an up-to-date Risk Management Plan that addresses all security and privacy risks
Cost and Schedule Performance	Planned costs, schedule and performance milestones indicate security as necessary

Table D-1. Exhibit 300 Security Requirements

In order to successfully address the Security and Privacy area of the Exhibit 300, each question in this section must be addressed at the system/application level, not at a program or agency level. For IT investments under development, security and privacy planning must proceed in parallel with the development of the system(s) to ensure that information security and privacy requirements and costs are identified and incorporated into the overall life cycle of the system(s). All IT investments must have up-to-date security plans and be fully certified and accredited prior to becoming operational. Having an interim authority to operate (IATO) is not acceptable by OMB's standards for the Exhibit 300.

Exhibit 300s are required to receive at least a "4" in the Security criteria and at least a "3" in the Privacy criteria. Investments that do not receive these minimum scores will fail and be placed on OMB's Management Watch List, regardless of the overall score received by the Exhibit 300.

Question 1: Have the IT security costs for the system(s) been identified and integrated into the overall costs of the investment?

This question requires a "Yes" or "No" response. IT security costs should always be identified and integrated into the overall costs of the investment.

Question 1a: If "yes," provide the "Percentage IT Security" for the budget year.

[21] OMB Circular A-130, Management of Federal Information Resources

This question requires a percentage response.

Federal agencies must consider the following criteria to determine security costs for a specific IT investment: the products, procedures, and personnel (federal employees and contractors) that are primarily dedicated to or used for provision of information security for the specific IT investment. Do not include activities performed or funded by the agency's IG.

When determining the percentage IT security include the costs of:

- Contingency planning and testing;
- Risk assessment;
- Security planning and policy;
- Computer security investigations and forensics;
- Specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security);
- Authentication applications;
- Cryptographic applications;
- Education, awareness, and training;
- System reviews/evaluations (including security control testing and evaluation);
- Oversight or compliance inspections;
- Development and maintenance of agency reports to OMB and corrective action plans as they pertain to the specific investment;
- Physical and environmental controls for hardware and software;
- Auditing and monitoring;
- Reviews, inspections, audits and other evaluations performed on contractor facilities and operations; and,
- C&A.

Question 2: Is identifying and assessing security and privacy risks a part of the overall risk management effort for each system supporting or part of this investment?

Identifying and assessing security and privacy risks should be a part of the overall risk management effort for every system.

Question 3: Systems in Planning and Undergoing Enhancement(s) – Security Table

All investments listed as Planning, Full Acquisition, or Mixed Life Cycle must complete this table. This table is used to identify all planned systems and/or planned enhancements to existing systems.

For each planned system and/or enhancement:

- Identify the name of the system;
- Indicate if the system is operated by the agency, contractor or both;
- Provide the planned operational date; and,
- Provide the planned C&A date.

A C&A with an Authority to Operate (ATO) is required for all systems before they may become operational; therefore, it is expected that the planned C&A date be before the planned operational date.

Question 4: Operational Systems – Security Table

All operational systems supporting the investment must be listed in this table. Systems identified in this table must be included in the agency's FISMA inventory and should be easily referenced in the inventory (i.e., should use the same name or identifier.)

For each operational system:

- Identify the name of the system;
- Indicate if the system is operated by the agency, contractor or both;
- Identify the NIST FIPS 199 Risk Impact Level;
- Indicate if C&A has been conducted using NIST SP 800-37;
- Provide the date C&A was most recently completed;
- Indicate the standards used for testing security controls;
- Provide the date the security controls were most recently tested; and,
- Provide the date the IT Contingency Plan was most recently tested.

C&A needs to be based on FIPS impact level and NIST guidance (800-37, FIPS 199, FIPS 200, 800-53) with very few exceptions. Per OMB Circular A-130, Appendix III, a C&A is required at least once every three years or when a major change occurs. Both security controls and the IT Contingency Plan are required to be tested at least annually.

Therefore, OMB expects:

- A C&A date, less than 3-years old (as of two weeks prior to the budget submission date) for all operational systems that are part of the investment;
- Security controls tested within the past year (365 days) for all operational systems that are part of the investment; and,
- Contingency plan testing within the past year (365 days) for all operational systems that are part of the investment.

Question 5: Have any weaknesses, not yet remediated, related to any of the systems part of or supporting this investment been identified by the agency or IG?

This question requires a "Yes" or "No" response.

If the operational systems that are part of the investment have any open weaknesses, the response to this question should be "yes."

Question 5a: If "yes," have those weaknesses been incorporated into the agency's plan of action and milestones process?

This question requires a "Yes" or "No" response.

If the weaknesses have been included in the agency's POA&M, the response to this question should be "yes." Note: all security weaknesses are required to be reported in the agency's POA&M.

Question 6: Indicate whether an increase in IT security funding is requested to remediate IT security weaknesses?

This question requires a "Yes" or "No" response.

If weaknesses have been identified and additional funding is required to address those weaknesses, the response should be "yes."

Question 6a: If "yes," specify the amount, provide a general description and explain how the funding request will remediate the weakness.

Provide the dollar amount required to remediate weaknesses and describe how the funding will be used to address the security weaknesses.

Question 7: How are contractor security procedures monitored, verified and validated by the agency for the contractor systems above?

If one or more of the associated FISMA systems (i.e., the systems listed in Tables 3 and/or 4) are contractor-operated/accessed, then an response is required for this question. The response should be specific to the investment and not boilerplate.

Question 8: Planning and Operational Systems – Privacy Table

Each system that is listed in the Systems in Planning and Undergoing Enhancement(s) Security Table and/or the Operational Systems Security Table, must also be listed in the Privacy Table.

For each system:

- Indicate if it is a new system;
- Indicate if there is at least one Privacy Impact Assessment (PIA) that covers the system;
- If a PIA does exist, provide the Internet link to the publicly posted PIA; if a PIA does not exist, provide an explanation why the PIA has not been publicly posted or why the PIA has not been conducted;
- Indicate if a System of Records Notice (SORN) is required for the system; and,

- If a SORN is required, provide the Federal Register Internet link for where the SORN may be accessed; if the response is "no," provide an explanation why the SORN has not been published or why there isn't a current and up to date SORN.

Appendix E. Case Study – Implementing NIST SP 800-65, Rev. 1 Guidance

The following sections provide an example of how the guidance presented in NIST SP 800-65, Rev. 1 may be implemented at an agency to select and fund security considerations. The example and accompanying descriptions highlight practices that are used at a variety of federal agencies. The information presented in this appendix is not compulsory; rather, it is one example of how agencies can implement the materials in this guidance document. Agencies should use the information provided in this guidance and customize it to their own operating environments to achieve maximum benefits.

E.1 Developing Prioritization Criteria Approach

The prioritization scheme used to rank order security investment considerations is usually established at the agency-level. Ideally, through a facilitated working session, the CIO, senior security officials, key system owners, and members of the Investment Review Board (IRB) identify information system investment prioritization criteria and each criterion's weight. A decision-support tool can be used to help the group enhance the quality of their decisions by using a sequential, pair wise comparison:

- Each participant identifies the criteria he/she feels is the most important in deciding which security needs should be funded.
- All criteria identified are presented to the group.
- With the assistance of the facilitator and the decision-support tool, the group then "votes" on the criteria and selects the criteria that will be used in the prioritization scheme.
- Once the criteria is identified, each participant then assigns a weight to each criterion to represent the priority that should be placed on that particular criterion.
- Similar to the process used for selecting the criteria, the weights are then shared with the group.
- With the assistance of the facilitator and the decision-support tool, the group "votes" on the weight.
- During the voting sessions, discussions occur to allow each participant to communicate his/her priorities.
- The end result is a prioritization scheme that is built on consensus and may be used throughout the agency.

Once the prioritization scheme is finalized, the agency produces guidelines for how the framework will be applied. The prioritization framework guidance identifies the parties that should be involved with making decisions at both the enterprise and system levels and provides recommendations for a scoring mechanism. The prioritization scheme and guidance is then shared throughout the agency.

E.2 System-Level Decisions

System-level decisions for investments in the Control and Evaluate phases of the investment lifecycle involve determining the management, operational, and technical controls that will be funded for a specific

information system. An example of such a decision would be reviewing the agency's POA&M and determining which corrective actions will be funded. The prioritization scheme is used when, due to budget constraints, it is necessary to choose between corrective actions.

The prioritization scheme may also be used to rank the security needs of one system or multiple systems. Depending upon the number of systems and/or the number of security weaknesses, the agency (or an operating unit within the agency) may need to consider each system separately and decide on a system-by-system basis which corrective actions will be funded. In other cases, the security needs of multiple systems may be reviewed and ranked collectively.

The individuals involved with the prioritization ranking of the security needs must have a comprehensive understanding of both the business and security needs of the system. At a minimum, the following individuals should be included in the process:

- System owner;
- Program/project manager;
- Information System Security Officer (ISSO);
- Technical lead/engineer; and,
- Budget analyst.

Once the "team" ranks the security needs and identifies those that will be funded first, the authorizing official, or other authorized individual or committee, reviews and approves the ranking.

During the decision making process, the decision team must determine if the security needs will be funded through the system's current budget, a reallocation of existing resources, or a new funding request. The system/program's budget analyst provides the team with the information necessary to make this decision. Once both the resources required to implement the corrective action and the funding source of those resources are identified, the agency's POA&M can be updated with this information.

If new funding is required for the security needs, it is included in the agency's annual budget request. The Exhibit 53 for the system (and if a major investment, the Exhibit 300) is adjusted to include the additional funding request.

E.3 Enterprise-Level Decisions

An enterprise-level decision involves selecting the security needs that will be funded to improve the agency's overall security posture. In most situations, this will involve investing in a new initiative or technology that will span the entire enterprise as opposed to a system or group of systems. The key personnel involved in enterprise-level decision are the investment owner and the IRB.

As referenced in Section 3.4.2, the enterprise investment's owner typically develops a concept paper for review by the IRB that provides a high-level description of the proposed investment and includes a rough-order-of-magnitude costing estimate, benefits, milestones, and agency impacts. Once the concept paper is approved, the investment owner develops a comprehensive business case to enable decision-makers to consider the potential of several investment alternatives before making an acquisition decision. With the results of the BCA, the IRB can make a justified selection of a preferred alternative for investment. Once business case is approved by the IRB, the agency must include it in the agency's IT investment portfolio and summarize the results of the BCA in the Exhibit 300.

E.4 Putting the Pieces Together: A Notional Scenario

An agency must decide between three competing IT security priorities in the fiscal year:

1. Implementing an unfunded mandate that requires implementation within the next two years;
2. Enhancing Network Access Controls to address a material weakness; and,
3. Acquiring a tool to analyze audit trails.

The CIO, senior security officials, key system owners, and technical advisors meet to review and rate these three competing security needs. The team evaluates each security need against the criteria and weights identified in the agency's prioritization scheme and assigns a "value score." The results are shown in Table E-1.

Note: The criteria and weights are identified in the agency's prioritization scheme. The weighted value score is the sum of each criteria's value score assigned by the team multiplied by the weight identified in the agency's prioritization scheme.

Prioritization Scheme		Security Needs Assessment: Value Score		
Criteria	**Weight**	**Unfunded Mandate**	**Network Access Controls**	**Audit Trail Tool**
Threat/Impact	High (3)	High (3)	Medium (2)	Low (1)
Likelihood	Low (1)	Low (1)	Medium (2)	Low (1)
Cost	Medium (2)	Low (1)	Medium (3)	High (3)
Cost-Effectiveness	High (3)	Low (1)	High (3)	Medium (2)
Feasibility	High (3)	Low (1)	High (3)	High (3)
Agency's Mission	High (3)	High (3)	Low (1)	Low (1)
Weighted Value Score		**27**	**33**	**28**

Table E-1. Notional Value Scores

Justifications for Security Needs Assessment Value Scores are provided in Table E-2 through Table E-4.

Unfunded Mandate		
Criteria	**Value Score**	**Justification**
Threat/Impact	**High (3)**	Personally identifiable information is at risk of being exploited; if exploited, the impact will be significant
Likelihood	**Low (1)**	Other security mechanisms are in place to protect against the threats, reducing the likelihood of exploitation
Cost	**Low (1)**	Acquisition and implementation are expected to be costly
Cost-Effectiveness	**Low (1)**	The initiative will only address a Federal mandate and does not provide a solution for other security requirements
Feasibility	**Low (1)**	The technology required to implement the mandate is in its infancy; available products do not meet the mandate's requirements
Agency's Mission	**High (3)**	The mandate is a Federal requirement

Table E-2. Unfunded Mandate Justification

Network Access Controls		
Criteria	**Value Score**	**Justification**
Threat/Impact	**Medium (2)**	Unauthorized access to the agency's network and devices may be obtained; if exploited, sensitive data is at risk
Likelihood	**Medium (2)**	It is fairly likely that the threat will be exploited
Cost	**Medium (2)**	Acquisition and implementation costs are expected to be moderate
Cost-Effectiveness	**High (3)**	Improving Network Access Controls will address security weaknesses found in numerous FISMA systems
Feasibility	**High (3)**	The technology required to enhance the network access controls is highly available
Agency's Mission	**Low (1)**	While security is always a priority, the investment does not directly support the agency's mission

Table E-3. Network Access Controls Justification

Audit Trail Tool		
Criteria	**Value Score**	**Justification**
Threat/Impact	**Low (1)**	Access to data and applications may be misused; if exploited, there is an impact to the agency, but it is not as significant of an impact as that presented by the threats the two competing security initiatives will protect against
Likelihood	**Low (1)**	There is a low probability of the threat being exploited
Cost	**High (3)**	Acquisition and implementation costs are relatively low compared to the competing two security initiatives
Cost-Effectiveness	**Medium (2)**	A tool will improve the agency's ability to analyze audit trails and detect misuse; this will address several security weaknesses related to the misuse of access and the integrity of data
Feasibility	**High (3)**	The technology required to analyze audit trails is highly available
Agency's Mission	**Low (1)**	While security is always a priority, the investment does not directly support the agency's mission

Table E-4. Audit Trail Tool Justification

After assessing the security needs and calculating a weighted value score, the stakeholders rank-order the initiatives. In this scenario, the priority is to fund the Network Access Controls first, then the Audit Trail Tool, and finally the Unfunded Mandate.[22] The stakeholders agree to the outcome and decide to proceed with seeking funding for the Network Access Controls initiative.

The next step is to develop a business case for the initiative. A project team is assigned to developing the business case. The team consists of individuals with skills in the following areas: Project Management, Acquisition, Budget, Cost Estimating, Enterprise Architecture, Performance, Risk Management, Scheduling, Technical expertise, and Earned Value Management.

The project team prepares a business case that addresses the following:

[22] Note: Though the first initiative is a mandate, in the notional scenario, it received the lowest score due to its high cost, low feasibility and low likelihood. The technology currently available in the market is in its infancy and cannot address all the requirements of the mandate. As the agency has two years to implement the mandate, it would not be a wise decision to allocate funding at this time to an investment that cannot meet the agency's needs. This initiative will remain an open security need and will be re-evaluated in the near future in compliance with the two-year timeframe.

- A description of the initiative, the benefits to the agency if funding is provided, and a summary of the funding requested for development, acquisition/implementation and maintenance for the entire life cycle of the investment;
- The investment's alignment to the agency's strategic goals and objectives and its ability to support Congressional mandates, material weaknesses, and/or audit findings;
- The business and technical requirements of the initiative;
- An alternatives analysis (to include a cost benefit analysis and a risk-adjusted Return on Investment and Net Present Value);
- An Acquisition Strategy tailored to the chosen alternative;
- A Risk Management Plan to assess the overall risks of the investment and identify how those risks will be mitigated;
- Performance measures that are tied to OMB's Performance Reference Model (PRM);
- A project plan that includes estimated costs and resources for each task listed within the Work Breakdown Structure (WBS); and,
- The investment's alignment to the Enterprise Architecture.

Once the business case is developed, it is presented to the assessment team for review and approval. Upon the assessment team's approval, the business case is provided to the IRB to be considered for inclusion in the agency's IT investment portfolio. The IRB reviews the business cases of all proposed investments and selects the ones that will be included in the agency's portfolio and submitted to OMB for inclusion in the President's Budget. An Exhibit 300 is prepared for all investments that are selected by the IRB and are defined as major by either OMB's or the agency's criteria.