2.0 ROLES AND RESPONSIBILITIES

This handout describes applicable roles and responsibilities for the Capital Planning and Investment Process (CPIC) as presented in the NIST *Integrating IT Security into Capital Planning and Investment Process Workshop*. It includes a discussion of roles and responsibilities of stakeholders in the various organizational models within federal agencies.

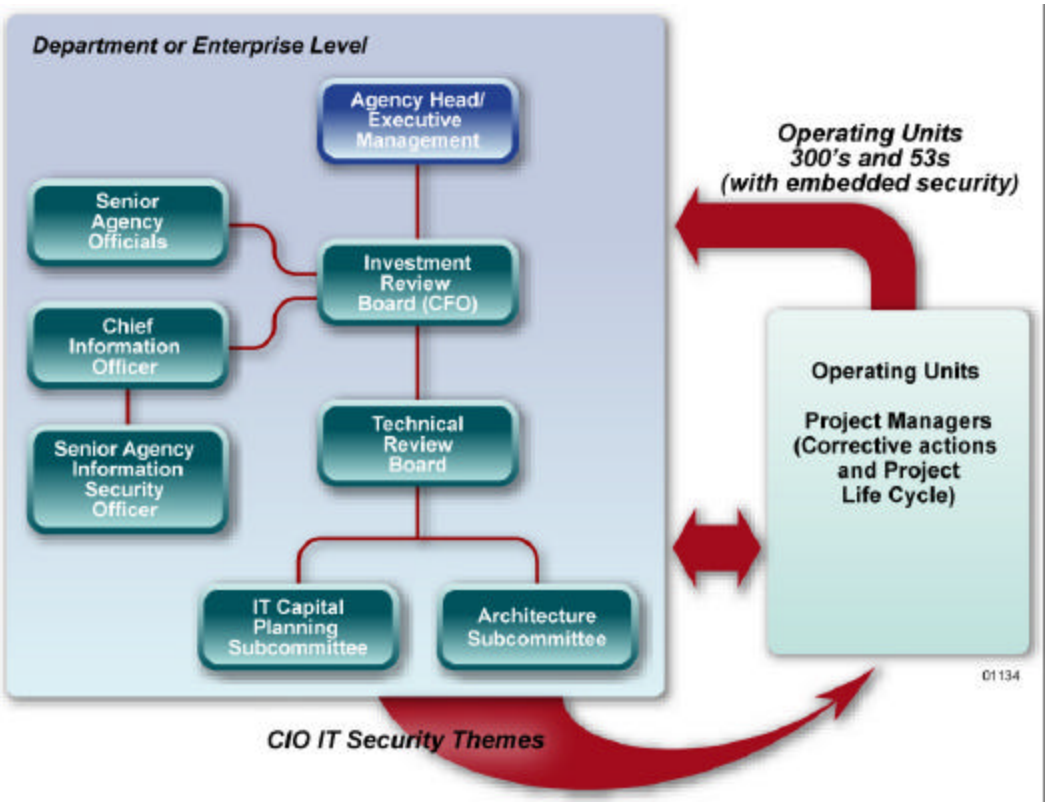

Figure 2-1. IT Management Hierarchical Diagram

2.1 Head of Agency

The head of the agency is accountable for the security posture of the organization's information technology (IT) infrastructure and is ultimately responsible for completing and submitting annual reports. This position controls both the security policy and the resource budget and has final management responsibility for resource allocation. The head of the agency has the following responsibilities related to integrating IT security into the IT CPIC process—

- Complying with the Federal Information Security Management Act (FISMA) requirements and the related information resource management policies and guidance including Office of Management and Budget (OMB) Circular A-130,

established by the Director of OMB, and the related IT standards promulgated by the Secretary of Commerce

- Ensuring the information security and resource management policies and guidance established are integrated with agency-strategic and operational planning processes under FISMA and are communicated promptly and effectively to all relevant officials within their agency
- Supporting the efforts of the director and the administrator of the General Services Administration to develop, maintain, and promote an integrated Internet-based system of delivering Federal Government information and services to the public
- 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 missions and vision (establish goals that flow down to budget, IT, and security themes) and ensuring that information security management processes are seamlessly integrated into those processes and documents
- Ensuring that the information protection is commensurate with the 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 Investment Review Board (IRB) process
- Establishing priorities to achieve improvements in compliance to the President's Management Agenda.

2.2 Senior Agency Officials

Senior agency officials provide information security for the information and information systems that support the operations and assets under their control, under the direction of the head of the agency. These 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 systems under their control
- Determining the levels of information security appropriate to protect 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 they are effectively implemented

- Delegating to the agency Chief Information Officer (CIO) the authority to ensure compliance with agency security requirements
- Providing senior IT advice to the head of each agency and the Management Review Board.

2.3 Chief Information Officer

The Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act) requires agencies to appoint CIOs. The agency CIO is the senior IT advisor to the IRB and the head of the agency. In this capacity, the CIO—

- Assists senior agency officials with IT issuesDevelops and maintains an agency-wide information security program
- Develops and maintains risk-based information security policies, procedures, and control techniques
- Designates a senior agency information security officer to carry out CIO directives as required by FISMA
- Designs, implements, and maintains processes for maximizing the value and managing the risks of IT acquisitions
- Presents proposed IT portfolios to the IRB
- Provides final portfolio endorsements
- Presents and recommends control and evaluates decisions and recommendations
- Ensures IT training for agency staff and oversees IT security personnel.

2.4 Senior Agency Information Security Officer

As mandated by FISMA, the senior agency information security officer is appointed by the CIO and manages information security throughout the agency. The senior agency information security officer is responsible for coordinating program requirements throughout the agency with designated points of contact and project managers, including—

- Developing and maintaining an agency-wide information security program
- Issuing annual IT planning guidance, including security themes, objectives, and prioritization criteria for new and legacy systems.
- Developing and maintaining information security policies, procedures, and control techniques
- Assisting senior agency officials concerning their responsibilities.

2.5 Chief Financial Officer

The agency chief financial officer (CFO) is the senior financial advisor to the IRB and the head of the agency. In this capacity, the CFO is responsible for—

- Reviewing 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
- Forwarding investment assessments to the IRB.

2.6 Investment Review Board

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. The IRB—

- Is composed of the CFO and organization and bureau management
- Operates at the enterprise level
- Approves the CIO's IT strategic guidance, including security themes and prioritization criteria (these themes and criteria need to reflect the evolving needs to security)
- Approves the controls and evaluates the IT portfolio with embedded security requirements, objectives, measures, and milestones
- Ensures alignment of President's Management Agenda (PMA) achievement, strategic agency missions, and vision with IT security themes and criteria.

2.6.1 Technical Review Board

The Technical Review Board (TRB) is comprised of OCIO elements (cyber security and architecture plus others), managers, and other applicable members. In this capacity, the TRB—

- Conducts detailed IT investment review and security analysis and reviews business cases for security requirements
- Balances IT investment portfolios based on CIO/IRB IT security themes and prioritization criteria
- Acts as a Department focal point for coordinating OCIO strategic planning, architectural standards, and outreach to organizations and bureaus.

2.6.2 IT Capital Planning and Architecture Subcommittees

Responsibilities of the IT Capital Planning and Architecture Subcommittees are to—

- Provide expertise on areas from OCIO and Operating Units, and as subject matter experts, perform an advisory function
- Translate OMB IT capital planning security guidance into operational and internal process control enhancements
- Supply process improvements and provide Enterprise Architecture support for the Technical Review Board.

2.7 Operating Unit Executive Management

Operating Unit Executive Management focuses on processes for integrating IT security themes into business cases and the OMB Exhibit 53/300 process.

2.8 Project Manager/System Owner

The project manager has overall responsibility for coordinating the management and technical aspects of the life cycle of a system. Responsibilities of a project manager may include (but are not limited to) 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
- Presenting, when appropriate, the progress of critical projects to the OCIO, the IRB, and other applicable review entities.

The system owner is located within the bureau/operating unit benefiting from or requesting the systems project/investment and is frequently thought of as the "customer" for that project. The system owner performs the following functions—

- Maintains active senior-level involvement throughout the development of the system
- Participates in project review activities and reviews project deliverables
- Coordinates activities with the agency senior IT executive

- Obtains and manages the budget throughout the project's life cycle against a project manager’s delivered, locked baseline
- Holds review and approval authority for ensuring that developed products incorporate security and meet user requirements
- Provides baseline assessment performance measures to evaluate the security of the delivered IT initiative.