United States
National Labor
Relations Board

Information Technology Strategic Plan (ITSP)

FY 2006–FY 2010

EXECUTIVE SUMMARY

This document describes the National Labor Relations Board's (NLRB) high-level information technology strategy and how that strategy will drive specific development activities. The Information Technology Strategic Plan (ITSP) is structured in the following manner:

Section 1, Overview, outlines the purpose of the plan and the legislative and policy directives that influence the plan. It also describes how the plan is structured and discusses the assumptions and constraints considered when creating the plan.

Section 2, NLRB Mission and Organization, provides a description of NLRB's mission and organizational structure, the future challenges that NLRB expects to face, and how those challenges will be addressed through its strategic information technology investments.

Section 3, High-Level Information Technology Strategies, provides an overview of NLRB's strategic vision for information technology. The high-level strategies include:

- Modernize Business Systems
- Enhance Enterprisewide Planning
- Maintain Currency with "Best Practices"
- Provide a Secure and Robust Infrastructure

Section 4, Major Technology Initiatives, shows how the high-level strategies will drive specific development activities.

SUMMARY OF CONTENTS

TABLE OF CONTENTS

1. OVERVIEW

During meetings with the NLRB CIO, Associate CIO's, and senior staff of the Program Management Office (PMO) the following IT strategic vision and supporting set of strategic goals were formulated. The staff began with the strategic goals of the Agency: (goal 1) *to resolve questions concerning representation promptly,* and (goal 2) *to investigate, prosecute, and remedy cases of unfair labor practices by employers or unions promptly*. Consequently, OCIO has made it its vision, *to deliver the right information and services to the right people at the right time, at any location.*

The strategic framework presented in this plan was developed through this process, and will be implemented through the building of business cases vetted and approved by the NLRB Investment Review Board (IRB).

1.1 Purpose of the Plan

The purpose of NLRB's Information Technology Strategy Plan (ITSP) is to improve the management, planning, and implementation of NLRB's information technology initiatives. The primary role of information technology is to support the business objectives of NLRB and to help the organization provide effective services to citizens. The ITSP provides a foundation for the development of the IT infrastructure and standards that are critical to ensuring the interoperability, consistency, and more effective management of training and support costs.

Overall, the ITSP provides guidance for NLRB to ensure that its information technology strategic initiatives align with the organization's mission and strategic objectives. The vision for information technology use at NLRB includes the development of an enterprisewide focus to the application of IT, a focus on serving the customer and an emphasis on enabling business process reengineering efforts.

1.2 Vision and Goals

The NLRB vision implies a fundamental reorientation of the role of Information Technology (IT) within the NLRB. The vision shifts the paradigm. IT will no longer be simply a support service, but an active catalyst for change and a direct contributor to mission accomplishment. IT will be an integrated, cohesive endeavor that builds on shared mission requirements and fosters a collaborative management environment. IT will no longer only match technology to identified business needs, but will proactively apply new and emerging technologies in support of the NLRB mission.

The Agency has established broad IT goals:

- Share information quickly, easily, and appropriately, inside and outside of the Agency—anytime and anywhere.
- Secure and protect information.
- Provide reliable, trusted, and cost-effective IT services.
- Use IT to improve program effectiveness and performance.
- Provide one-stop shopping to citizens through the use of portal technology.

To meet these goals, the NLRB is initially focused on key areas that constitute the core building blocks of the Agency's IT program. This plan outlines these areas and presents specific initiatives for action.

1.3 Key Assumptions and Constraints

A variety of organizational, economic, and technical assumptions and constraints were considered when formulating this strategy.

1.3(a) *Organizational*

- NLRB is a mission-focused organization whose core business applications must remain tightly aligned with the business functions. Updating the business applications and infrastructure to more cost-effectively support the business function is the objective of every major IT initiative.

- Alignment of information technology initiatives and Agency strategy will involve the participation of key agency decision makers.

- Improved understanding of information technology will help NLRB decision-makers identify and prioritize the service improvement initiatives.

- OCIO will provide background information, alternatives and recommendations to educate the business customers on the impacts of their initiatives, and their associated risks. A partnership between the business units and OCIO will help bi-directional communications. Business units must not only understand that IT expenditures benefit them, but that they are also responsible for prioritization of initiatives across the agency.

- Care must be taken to ensure that the needs of the entire organization are captured, and solutions are developed that reflect a corporate/unified approach and execution of the Agency's mission.

- To ensure efficient operations within OCIO, clear lines of responsibility and accountability over specific functions must be drawn and communicated to employees.

1.3(b) *Economic*

- Adequate budget resources are required to maintain current service levels, while meeting the additional challenges involved in improving planning processes, creating E-Government pilot projects, and meeting new and expanded Federal mandates.

- NLRB must have enough flexibility in its IT budget to comply with new requirements and to cover unforeseen costs.

- NLRB will plan in advance to ensure budgets reflect future needs.

1.3(c) *Technical*

- NLRB will expend resources to replace outdated systems, architectures, and infrastructure.

- OCIO will continue to align Information Technology program execution with the business goals and objectives of the Agency.

- OCIO staff will continue to maintain an up-to-date knowledge of current technology through on the job and formal training.

- NLRB will continue to work toward full implementation of structured development methodologies for all custom and packaged Agency systems.

- NLRB will continue with its efforts to build and evolve its “To-Be” business and technical architecture.

- NLRB is currently breaking down its technology stovepipes. All new applications will use current technology, e.g., web-based and open standards Commercial Off-the-Shelf (COTS) packages to maximize user functionality and minimize maintenance costs.

- NLRB will maintain a high degree of application and platform standardization across the Agency, where similar functions/automation requirements exist. These common applications/platforms will be selected to support standardization of functions and processes, and to minimize application support costs.

- NLRB will mitigate internal and external security threats.

- NLRB will support open standards as a general rule.

- Business applications will be built using a Service Oriented Architecture (SOA) framework.

2. NLRB CURRENT ENVIRONMENT

The National Labor Relations Board is an independent Federal agency created by Congress in 1935 to administer the National Labor Relations Act, the primary law governing relations between unions and employers in the private sector. The statute guarantees the rights of employees to organize and to bargain collectively with their employers or to refrain from all such activity. Generally applying to all employers involved in interstate commerce—other than airlines, railroads, agriculture, and Government—the Act implements the national labor policy of assuring free choice and encouraging collective bargaining as a means of maintaining industrial peace. Through the years, Congress has amended the Act and the Board and courts have developed a body of law drawn from the statute.

NLRB's mission is (1) to determine, through secret-ballot elections, the free democratic choice by employees whether they wish to be represented by a union in dealing with their employers and if so, by which union; and (2) to prevent and remedy unlawful acts, called unfair labor practices by either employers or unions. The Agency does not act on its own motion in either function. It processes only those charges of unfair labor practices and petitions for employee elections that are filed with NLRB in 1 of its 51 Regional, Sub regional, or Resident Offices.

2.1 Challenges Ahead

NLRB expects to face several challenges over the next few years. The Information Technology Strategic Plan (ITSP) describes the NLRB's planned information technology investment initiatives. It will enable the Agency to successfully address these challenges:

- **Rapidly Changing Technology**
- **Increasing Customer Expectations**
- **Federal IT Mandates and Initiatives**
- **Technology Budget**
- **IT Security**

2.1(a) *Rapidly Changing Technology*

The rapid pace of technological change is a challenge every private and public sector organization faces. NLRB recognizes the speed at which these technological advancements are occurring and realizes the importance of addressing this challenge. NLRB understands that information technology is critical to reaching its strategic goals and activities. Nearly every activity relies on technology to disseminate information and collect data. To meet this challenge, NLRB plans to update its systems and architecture to keep pace with these changes.

Meeting and exceeding customer expectations is a vital objective for NLRB's OCIO, and through its E-Government strategic initiative, NLRB is improving service to its citizens, employees, and other organizations it serves. E-Government is important to NLRB, not only because it is federally mandated, but more importantly because it promises to bring NLRB's data closer to customers and stakeholders as a way of continuing to improve service to citizens.

2.1(b) *Federal IT Mandates and Initiatives*

All Federal agencies are required to meet the information technology requirements mandated by Congress. NLRB faces the challenge of implementing these regulations, including the Government Performance Results Act of 1993 (GPRA), the Clinger-Cohen Act, Federal Information Security Management Act (FISMA), and E-Government. For instance, NLRB must be able to measure the performance of its IT investments, consistent with the GPRA and the Clinger-Cohen Act. ***Furthermore, the Clinger-Cohen Act requires that business processes be streamlined, redesigned, or eliminated prior to investing in information technology to support them*.** The directive is focused on business process improvement and not simply applying new technology to old processes.

NLRB will meet this challenge through its strategic IT Governance processes and Investment Review Board (IRB). It will evaluate proposed project business cases and use a performance-based portfolio management system to evaluate investment alternatives, determine feasibility, and track performance metrics of individual IT projects. Enterprise Architecture will be used as the roadmap to realign and re-engineer processes to best meet the needs of citizens, other agencies, businesses, and Federal employees.

2.1(c) *Information Technology Budget*

In FY 2000, Congress appropriated $206M to support Agency operations while the Information Technology budget was funded at $11.75M. This represented approximately 5.7 percent of the total Agency budget. In FY 2006, Congress appropriated $252M while the Information Technology budget was funded at $9.6M which represented 3.8 percent of the total Agency budget. Since FY 2000, the Agency budget has grown just over 22 percent while the IT budget has been reduced 18 percent.

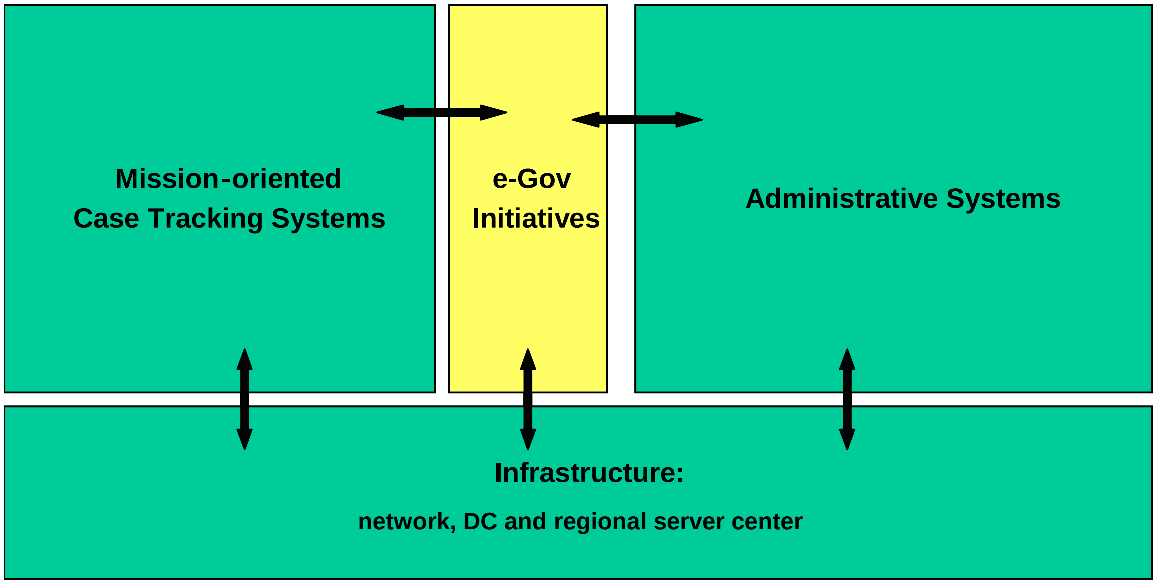
The future outlook of the NLRB budget doesn't look much better. It is expected that the Agency budget will be funded at or near FY 2006 levels for the foreseeable future putting additional pressure on the Agency to find ways to cut payroll and or leases, while at the same time find the necessary funding for Information Technology and quality of life items for the NLRB staff.

Key funding challenges for the OCIO include OMB mandated initiatives to transition to the Internet Protocol Version 6 (IPv6), Federal Information Systems Management Act (FISMA) compliance, and annual Life Cycle Management of IT components. Key funding challenges for the OCIO also include the transition to a Next Generation Case Management (NGCM) platform and the Chairman's e-Gov initiatives supporting the President's Management Agenda.

3. IT STRATEGIES

The figure below illustrates NLRB's key IT activities: the mission-oriented Case Tracking Systems; E-Government initiatives; the Administrative Systems; and the IT Infrastructure that supports all activities.

NLRB's Key IT Activities



Mission-oriented Case Tracking Systems

e-Gov Initiatives

Administrative Systems

Infrastructure:

network, DC and regional server center

The high-level strategies described below will guide the support of these activities for the next 5 years. Mission-oriented case tracking systems will evolve toward a single enterprise-wide environment for managing case information. E-Government initiatives will improve service to citizens and business. Key administrative systems have been cross-serviced through the department of Agriculture, National Business Center (NBC). Finally, strategies to enhance enterprise wide planning and provide a secure IT environment will focus on the infrastructure business process reengineering, as well as each of the key IT activities.

High-Level Strategy	Related Initiatives
Modernize Business Systems	• Next Generation Case Management (NGCM) • E-Government Portal • Enterprise Content Management (ECM)

Enhance Enterprise wide Planning	• IT Strategic Plan • Enterprise Architecture • Capital Planning • Acquisition Planning • Program Management Office
Provide a Secure and Robust Infrastructure	• FISMA Compliance • Contingency Planning • System Availability (Anytime, Anywhere) • Hardware Consolidation and Standardization • Wireless Technologies • IPv6 • Network Convergence
Maintain Currency with IT Best Practices	• ITIL • Lifecycle Management • Open Standards
Restructure Workforce/Succession Planning	• IDPs • Skill gap analysis

Overall, NLRB is moving from an environment where individual systems and capabilities are developed to support a single customer to an environment where enterprise planning determines the scheduling and priorities for both system development efforts and investments in the enterprise-wide infrastructure.

3.1 Modernize Business Systems

3.1(a) Next Generation Case Management

The vision for the NGCM project is to build an enterprise wide, common case management platform using the latest technologies for interfacing with the public and managing cases across NLRB's offices in an automated, efficient, and transparent way. The NGCM project will enable the Agency to replace or optimize manual, paper-based processes and stove-piped legacy systems with a standards-based solution leveraging COTS tools using a Service-Oriented Architecture (SOA) framework. The OCIO will deliver critical business services using a SOA framework.

The NLRB wishes to use technology to:

- Transform the way the NLRB does business with the public, making its cases transparent, more available to its customers in a timely matter. Enable the public to access online any documents associated with cases that may be disclosed under Freedom of Information Act (FOIA).
- Optimize internal NLRB case processing so NLRB employees can work smarter and faster.

- Provide Agency wide electronic case records and case document management to improve internal case flow, Agency readiness to provide electronic court filings and reference documents retrieval.

NGCM will replace the following case tracking and document archiving systems: Case Activity Tracking System (CATS), Pending Case List (PCL), Trial Information Gathered on Electronic Records (TIGER), and Litigation Information on the Network (LION), among others. Judicial Case Management System (JCMS) and its underlying Documentum e-Room will remain. JCMS and NGCM will link to each other using a Service Oriented Architecture (SOA) framework.

The Agency has not predetermined the order and/or replacement of any of the legacy systems at this point. It is envisioned that the NLRB will work with the vendor on developing alternative strategies for replacing, optimizing, converting, integrating, and/or interfacing with these systems during the project. The key assumptions and high level business objectives are presented below.

The NGCM will integrate the key business functions, e.g., case management and tracking, electronic case files, and a customer relationship management function that includes a public-facing interface to initiate and track cases. The NGCM will have:

- A common case management platform for all components. NGCM will replace each component's legacy case management system and functionality.
- Workflow management capabilities that will allow cases, and parts of cases, to circulate from one office to another during the case life cycle. The extent of the workflow requirements will be determined during the detailed requirements phase and/or at later phases.
- Document management capabilities that will allow case documents to be edited and reviewed electronically by more then one person.
- End-user data entry capabilities with automated data validations and an underlying data integrity scheme and audit trail capabilities.
- Search and reporting capabilities that include but not limited to standard search algorithms, standard and customized reporting and executive summaries of the information in the system possibly with the aid of graphical tools to provide executive dashboard capabilities.

3.1(b) *Enterprise Content Management (ECM)*

The "official" definition of Enterprise Content Management (ECM) was coined by the Association of Imaging and Information Management (AIIM) international, the worldwide association for Enterprise Content Management in the year 2000. The acronym ECM has been reinterpreted and redefined many times during the past years, replacing words like "create" or "customize" that were originally part of it.

In autumn 2005 AIIM defined ECM as follows:

> Enterprise Content Management is the technologies used to Capture, Manage, Store, Preserve, and Deliver content and documents related to organizational processes.

Traditional archive, document management, and workflow functionalities from the document-related technologies field have been converted into or used to generate new product suites that combine web-based components with conventional products. In this context, content management generally becomes enterprise content management. This nomenclature is intended to demonstrate that it is not just about a company's web-oriented face to the outside world, but about all of the structured and unstructured information in the company. From this approach come new components that make useful additions to content management-automatic classification in corporate taxonomies, profiling, web transactions archiving, and more.

In the future, it is reasonable to assume that more and more legal artifacts will be in electronic format. Work documents, images, videos, and audio recordings may become part of the case file. Because of this, an ECM solution must be considered when migrating towards the Next Generation Case Management.

3.1(c) *E-Government Portal*

E-Government is a multi project effort to provide new, faster channels for NLRB's services to all of its customers through effective use of the Internet. The NLRB has already completed several initiatives to bring its services online. While this has proven to be a good start in the right direction, the systems are still disconnected from one another and exist as silos. An enterprise approach integrating key components of Next Generation Case Management, Enterprise Content Management, and a web (integration) portal will be needed to provide end-to-end content delivery to stakeholders and NLRB employees. E-Government is important to NLRB because it allows the work force to focus on its core competencies instead of manual communications processes.

NLRB's E-Government investment follows OMB's Government to citizen (G2C) initiative and promotes internal efficiency and effectiveness. With Enterprise Planning, E-Government investments will be screened and prioritized by the IRB.

Because the mission of NLRB focuses on serving citizens, the measure of success of the E-Government investment will be the degree to which NLRB has a virtually seamless convergence of on-line interaction with the public, business, other agencies, and its internal processes.

The portal will provide a single point of access to information across the Agency through a browser-based interface. The Portal will serve as a launch point for the various E-Government initiatives. The more important features of a portal include information organization, search capabilities, personalization, business intelligence, knowledge management, and application integration.

3.1(d) *Maintain Administrative Systems*

The OCIO will continue to support the Agency's administrative systems for finance, budget, procurement, and human resources management. We will continue to procure

Finance, Payroll, and Personnel systems support through the National Business Center (NBC).

3.1(e) *Strategic Justification*

The NLRB investigates allegations, conducts administrative hearings, and facilitates settlements in accordance with goal 2: to investigate, prosecute, and remedy cases of unfair labor practices by employers or unions promptly. The NGCM will serve a vital role in supporting the Agency's mission fairly, quickly, effectively, and efficiently.

NLRB's portal and E-Government initiative supports the mission and goals stated in its strategic plan. By using Enterprise Planning and the Capital Planning and Investment Control (CPIC) process, NLRB will be able to identify E-Government investments that will enable NLRB to meet its goals of conducting business faster by eliminating and streamlining existing processes through the use of technology.

E-Government will help resolve questions concerning case status promptly by inserting speed and efficiencies into the business processes. NLRB will use its Enterprise Planning initiative to identify and prioritize those areas best suited for E-Government. These areas will then be targeted for E-Government pilot projects.

3.1(f) *Alignment with the President's Management Agenda*

NGCM, the public-facing portal, and content management initiatives support the following strategic goals from the President's Management Agenda:

<u>Expanded E-Government:</u> NLRB's E-Government investment directly supports the President's priority on *Expanded Electronic Government*. NLRB expects E-Government to not only improve its internal and external interactions, but also to eventually help achieve seamless integration into a virtual one-stop-shop for government services, which is an important goal of the current administration.

Projects will target select business processes for reengineering. In performing these pilots, NLRB seeks to increase its understanding of how to manage such projects, and increase demand and acceptance for additional E-Government investments.

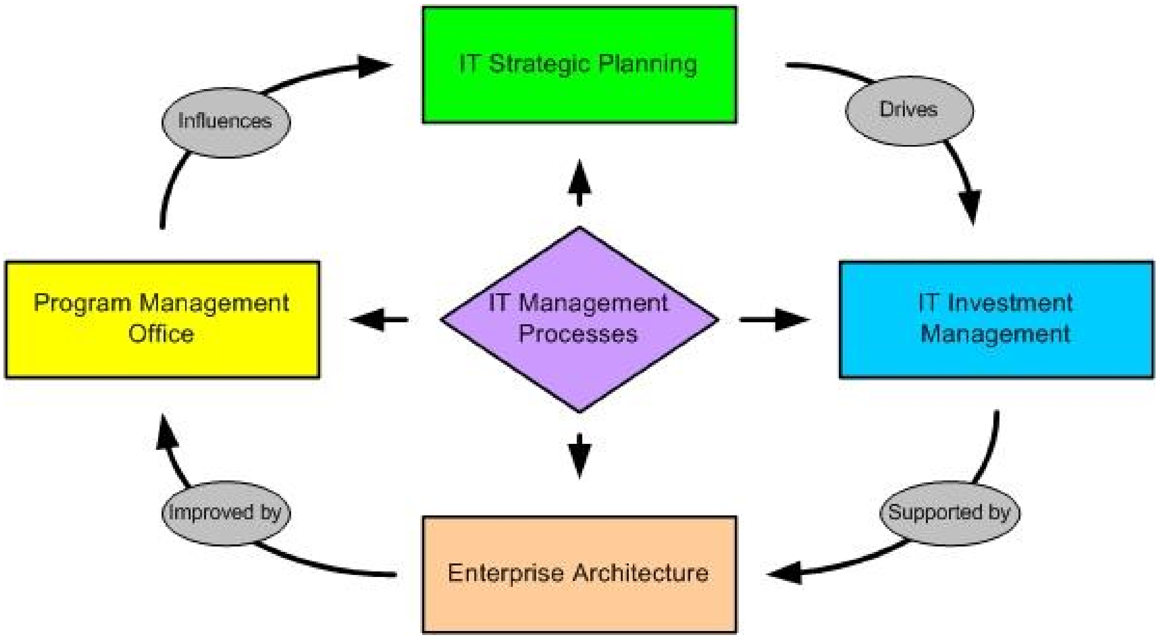
One goal of this investment will be to decrease costs by eliminating many of the existing manual processes, thereby reducing NLRB's dependence on clerical activities.

The NGCM and other enterprise application solutions, such as ECM, server consolidation, and e-filing, will unify data and documents stored across the NLRB business units. It will provide quick, and appropriate, access to documents, case files, and case status for NLRB employees and the public. It will also support the courts with electronic case materials.

By eliminating the need to support the various technologies supporting the legacy applications that will be replaced, the NGCM also supports the President's Management Agenda (PMA) efforts to streamline and modernize.

3.2 Enhance Enterprisewide Planning

The NLRB will integrate the Strategic Planning function with other IT management processes to ensure that project planning; funding, prioritization, and execution are in line with the principles, standards, and the IT architecture.



OCIO Strategic Management Framework

3.2(a) *Information Technology Strategic Plan*

The purpose of NLRB's ITSP is to synchronize future IT activities and resources. The ITSP provides guidance for NLRB to ensure that its strategic information technology initiatives align with the organization's mission and strategic objectives. The vision for information technology use at NLRB includes the development of an enterprise-wide focus to the application of IT, a focus on serving the customer, a focus on improving internal processes and procedures with an emphasis on enabling business process reengineering efforts.

3.3(b) *Enterprise Architecture*

The CIO Council defines Enterprise Architecture as "A strategic information asset base, which defines the mission, the information necessary to perform the mission, the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to the changing mission needs." Enterprise Architecture is an IT management process that translates business strategy into business value. The NLRB will use a collaborative process to create deliverables such as principles, guidelines, models, standards, and roadmaps to guide the development of new IT capabilities. These deliverables will shape the design choices for projects so they can work together to support the business strategy.

3.3(c) *Capital Planning and Investment Control*

With more formalized IT capital planning and investment control processes in place, NLRB has a comprehensive planning process that enables it to plan, select, and control IT investments, and evaluate the results.

The four phases of NLRB's CPIC process that will be integrated into the Enterprise Planning process are planning, selection, control, and evaluation. The planning and selection phases are outlined in the NLRB Investment Review Board (IRB) Charter. Following the Charter, the technical and business project managers present investment proposals to initiate new projects, and provide project updates for ongoing project evaluation. The IRB meets on a monthly basis and is comprised of seven senior level managers who manage the CPIC process of planning, selection, control, and evaluation process.

3.2(d) *Program Management Office (PMO)*

The goal of the PMO is to provide tools, methodologies, and resources to help OCIO project managers become more successful, and to streamline and automate many of the management tasks. The Program Management Office will provide:

- State-of-the-art project management software which will include automated project scheduling, project interdependency tracking, issue management, resource management, and other tools.
- Assistance in managing risks and addressing quality considerations.
- Skills training for project managers.
- Consistent and effective project management methodologies.
- Proactive communication of project and task status.

3.2(e) *Acquisition Planning*

To manage our IT acquisitions, OCIO has established a Program Management Office with emphasis on acquisition/program planning through developing and implementing improved acquisition:

- Program management policies, procedures, and guidance to IT Program managers/contracting officer’s representatives in compliance with Federal and Agency regulations.
- The acquisitions will be more performance based, meaning that the basis for IT requirements will be based on the Agency’s strategic plan—mission and program performance objectives.
- More emphasis on the market research and focusing on generating competition and innovation and the use of commercial and nondevelopmental items to meet mission needs and developing most suitable approach to acquiring needed supplies and services.
- More emphasis on risk management through monitoring and controlling performance, cost, and schedule objectives (earned value management) for contracts and internal projects.
- Establish Integrated Project Teams (IPT) and develop acquisition strategies for larger acquisitions.

3.2(f) *Strategic Justification*

The ITSP will serve as a tool for building more effective systems to meet NLRB's increasingly aggressive targets. Managers can use it and the Enterprise Architecture to help identify redundant and inefficient systems and processes that are not in alignment with the mission, and that are candidates for automation/redevelopment.

Enterprise Architecture and IT Capital Planning and Investment Control are tools and processes specifically designed for the purpose of reducing costs and improving efficiencies. Cost savings will be achieved through successful Enterprise Architecture implementation due to gains in efficiency through business process reengineering. The CPIC process will also help to align IT projects with the Agency's mission and strategic goals.

3.2(g) *Alignment with President's Management Agenda*

IT Strategic Planning, Enterprise Architecture, Capital Planning and Investment Control, and Program Management procedures directly support the following governmentwide objectives of the President's Management Agenda:

Improved Financial Performance. By promoting an enterprisewide view of systems development, the OCIO will be able to identify those systems and processes that are redundant, thus, improving the efficiency and effectiveness of the IT program. The planning process will identify ways to remove barriers and promote appropriate data sharing, while protecting proprietary data.

Project managers will be able to clearly identify those points where the NLRB's businesses processes and systems come in contact with outside processes of other organizations and individuals. The project managers will use enterprise planning as a roadmap to realign and reengineer processes to best meet the needs of citizens, other agencies, businesses, and Federal employees.

Budget and Performance Integration. As part of Enterprise Planning, NLRB will use performance objectives and measures for each investment entering the CPIC process. Those performance metrics will become an integral part of the PMO, which will measure performance of individual projects and assess feasibility.

3.3 Provide a Secure and Robust IT Infrastructure

3.3(a) *IT Security*

NLRB is dedicated to fully protecting its infrastructure and critical assets within the enterprise. The IT Security Officer is responsible for ensuring the development, implementation, and management of an agencywide IT security program. To ensure data confidentiality, integrity, and availability, the security program integrates:

- Policy that outlines the roles and responsibilities of each user.
- Procedures for secure operations of IT resources.
- Standards for the implementation and operation of applications across the Agency, as well as security guidelines for users to follow.

These functions are addressed in the IT security program structure.

Following guidance from the National Institute of Standards and Technology (NIST), and in accordance with FISMA, NLRB data sensitivity is designated ‘sensitive but unclassified’ (SBU). The NLRB has implemented an appropriate security program focusing on six elements:

- IT Security Program Evaluation and Development
- IT Security and Awareness and Training
- IT Certification and Accreditation
- IT Vulnerability Testing and Correction
- Contingency Planning
- Homeland Security Presidential Directive 12 (HSPD-12)

3.3(b) *Strategic Justification*

OMB and public laws require specific controls for IT systems that provide protection for individual privacy and data integrity. To obtain and maintain privacy and data integrity, NIST has been identified as the leading Agency for providing guidance on the development and implementation of Federal systems processing Sensitive But Unclassified (SBU) data. In accordance with OMB, NLRB processes, at a minimum, SBU information. To provide the minimum level of protection as required by OMB and recommended by NIST, NLRB developed an IT Security program that will follow the recommendations of NIST. NLRB will continue to look towards the private sector for assistance in the maintenance of the IT Security program and FISMA reporting requirements.

3.3(c) *IT Infrastructure*

3.3(c)(1) *System Availability*

The strategic focus for Infrastructure over the next several years will be to establish a readily available computing environment for NLRB employees and the public at large who need access to NLRB systems and information. Given that the OCIO government staff provide 5x8 coverage (excluding holidays), an external remote hosting service provider is needed to provide the additional coverage. As NLRB transitions toward E-Government and on-line applications, system uptime will be a critical success factor. Currently, if a system goes down on a weekend or after hours it is not repaired until the following Monday or next morning at the very earliest.

3.3(c)(2) *Hardware Consolidation and Centralization*

To provide effective access to NLRB systems and information, consolidation and centralization of systems into the hosting facilities will be necessary. Doing so will reduce overall costs and increase effectiveness. Costs will be lowered by reducing the number of servers required to support Regional/Resident offices and reducing operational costs for monitoring and maintaining the systems (hardware and operating system). Backups will be done centrally at the hosting facilities relieving the Regional Office staff of that responsibility.

3.3(c)(3) *Next Generation Internet Protocol (IPv6)*

IPv6 is short for "Internet Protocol Version 6". IPv6 is the "next generation" protocol designed by the Internet Engineering Task Force (ETF) to replace the current version, Internet Protocol, IP Version 4 (IPv4).

Most of today's internet uses IPv4, which is now nearly 20 years old. IPv4 has been remarkably resilient in spite of its age, but it is beginning to have problems. Most importantly, there is a growing shortage of IPv4 addresses, which are needed by all new machines added to the Internet. IPv6 fixes a number of problems in IPv4, such as the limited number of available IPv4 addresses. It also adds many improvements to IPv4. IPv6 is expected to gradually replace IPv4, with the two coexisting for a number of years during a transition period.

All Government agencies have been directed by the Office of Management and Budget to transition to Internet Protocol Version 6 compliant devices by June 2008.

3.3(c)(4) *Wireless Technologies*

The term wireless technology is generally used for mobile IT equipment. It encompasses cellular telephones, personal digital assistants (PDA's), and wireless networking. Other examples of wireless technology include Global Positioning Systems (GPS) units, wireless computer mice and keyboards, satellite television, and cordless telephones. The OCIO will continue to support its use of PDA’s which have the ability to access the Internet, intranets, or extranets via Wi-Fi, or wireless wide-area networks. Agency managers can synchronize to a personal computer with their PDA’s using Microsoft ActiveSync. Synchronizing PDA’s with personal computers ensures that the PDA has an accurate list of contacts, appointments, and e-mail, allowing users the same information on the PDA as their host computer.

3.3(c)(5) *Network Convergence*

Convergence describes a networking environment where voice, video, and data transmissions are integrated within a single, unified system. More specifically, this network is based on Internet Protocol (IP) standards, the same architecture that drives the World Wide Web. Network convergence enables an organization to use services like IP telephony (also called Voice-over-IP, or VoIP), unified messaging (voice and e-mail), videoconferencing, wireless communications, and a host of other applications that seamlessly integrate voice, video, and data communications.

Moreover, the converged network utilizes a "distributed" framework to provide this functionality to users. When deployed over a Wide-Area Network (WAN), data and application information for all services reside on centralized servers rather than terminal devices, and are distributed to the end user over the network to IP-enabled devices (e.g., IP phones). Again, it's the same architecture that supports the browser-based model common to the Internet. Perhaps most importantly, by consolidating the separate networking systems and services for voice, video and data, convergence means an organization has only one cost-effective, unified network infrastructure to design, deploy, manage, and support.

Network convergence is now mainstream technology and the next move should be to implement VoIP and replace the VTC contract with an integrated data, voice, and video network capable of supporting all three functions. To do so will require the NLRB to transition away from the MCI public data network and establish a private network capable of supporting convergence.

3.3(c)(6) *Strategic Justification*

New technology will continue to evolve and enable users to have faster access to more timely data, which will trigger demands to increase the use of information technology to help manage current programs and provide new services. It is essential that centralized network management activities are accomplished to improve the maintainability and availability of network resources; achieve the level of operational integrity required to support the processing needs and expectations of the customer community; and provide the necessary level of security.

Achieving standardization in the Agency's use of hardware and software, will allow for simplified management to accomplish the push of software upgrades, patches, and the deployment of new software packages throughout the enterprise. Infrastructure Support will transition the desktop environment to a Microsoft Business Desktop Deployment (MBDD) solution which will permit a zero-touch automated solution to desktop management for imaging, patching, software distribution, software metering, etc.

3.4 Information Technology Best Practices

The OCIO will implement tools and best practices that make routine tasks such as server administration, network troubleshooting, and desktop support less time consuming and burdensome, so that the IT staff can focus their energies more on strategic projects that add value to the NLRB.

3.4(a) *Information Technology Infrastructure Library (ITIL)*

Service management best practices enable organizations to get more value out of their IT investments, reduce IT costs, and improve alignment with business needs. The components of service management are: Incident Management, Problem Management, Configuration Management, Change Management, and Release Management.

The OCIO will move forward with its implementation of service management so that we are as smart and flexible in our use and deployment of technology as our customers are in the accomplishment of the Agency mission.

OCIO will ensure its staff has the technical skills as well as the operational strategies necessary to support the business of the NLRB. The Information Technology Infrastructure Library (ITIL) is the most widely accepted approach to IT service management in the world. ITIL provides a cohesive set of best practices, drawn from the public and private sectors internationally. It is supported by a comprehensive qualifications scheme, accredited training organizations, and implementation and assessment tools.

ITIL has been around for 20 years, but interest within the United States has only increased in the last 5 years. ITIL is becoming the next big thing in IT. It is the new industry buzzword, the new certification, and the new idea in the IT world. ITIL describes a framework of processes for the management of IT. Because it is a framework, ITIL does not describe in great detail how any particular process should be implemented.

3.4(b) *Lifecycle Management*

Lifecycle management is a process by which IT manages computing assets throughout their lifecycle and is essential for making informed technology-related business decisions, optimizing existing infrastructure, cutting support costs, and planning overall capital expenditures.

- The refresh period for personal computers will be 25 percent per year.
- Personal printers will be discarded if they break after the 1-year warranty period is over.
- Server refresh will take place on a predefined 3-5 year schedule depending on the mission criticality of the server and the applications installed.
- Annual software maintenance renewals will be reviewed 3 months prior to the end of the period of performance. The review process will decide whether there is still a requirement for the product and whether the license count is accurate.

3.4(c) *Open Standards*

“Open standards are publicly available specifications for achieving a specific task. By allowing anyone to use the standard, they increase compatibility between hardware and software components since anyone with the technical know-how and the necessary equipment to implement solutions can build something that works together with products of other vendors.” The OCIO will continue to employ open standards in its network protocol. The OCIO will also continue to use structured query language (SQL) (a specification approved by the American National Standards Institute (ANSI) and International Standards Organization (ISO); Internet Protocol (IP) (a specification of the Internet Engineering Task Force (IETF) for transmitting packets of data on a network; Transmission Control Protocol (TCP) (a specification of the IETF for implementing streams of data on top of IP), and Hypertext Markup Language (HTML) (specifications of the World Wide Web Consortium (W3C) for structured hyperlinked document formatting) in its open standards suite of tools.

4. MAJOR INFORMATION TECHNOLOGY INITIATIVES

This section describes NLRB's major information technology initiatives and how they relate to the high-level strategies discussed in the previous section. These investments will be the focus of information technology planning and implementation efforts over the next few years. They are critical to improving the efficiency and effectiveness of business operations.

NLRB's vision is to shift to an environment where enterprise planning determines the scheduling and priorities for both system development efforts and investments in the enterprise-wide infrastructure, as depicted in the graphic below. As mentioned previously, this manner of planning is needed to support the type of web-enabled, robust functionality envisioned for new systems at the Agency.

Timeline for Change

Year 1

Establish Enterprise Planning and consolidate infrastructure

- Implement JCMS stages 1 and 2 for ES and Board members
- Complete IT Strategic Plan
- Update Technical Enterprise Architecture
- Establish PMO
- Establish "east coast" remote server hosting contract
- Additional E-Government functionality (expanded E-Filing)
- Implement public facing web portal (personalization)
- Initiate NGCM
- Legacy application maintenance
- Initiate consolidation and centralization of regional server effort
- Assess IPv6 requirements
- Implement Primavera
- Annual life cycle replacement of servers, PCs, laptops, printers
- Establish remote access program

Year 2

Refine Enterprise Vision and Enhance Technology Platforms

- Build out JCMS for rest of Board offices
- Establish formal project management governance via Primavera
- Integrate E-Government initiatives into Portal
- Complete technical and business enterprise architecture
- Complete server consolidation (phase 1). Start phase 2
- Establish "west coast" remote server hosting contract
- Annual life cycle replacement of servers, PCs, laptops, printers
- NGCM pilot
- Complete portal
- Replace non-IPv6 components
- Expand remote access program
- Wireless pilot program

Years 3-5

Create IT-Enabled Processes

- Update Enterprise Architecture and Enterprise Planning process
- Complete NGCM
- Complete E-Government initiatives
- Complete JCMS
- Complete integration of NGCM, Enterprise Content Management, Portal, and JCMS.
- Maintain enterprise business systems and add functionality dictated by business requirements
- Competitively source non-governmental support functions
- Ongoing analysis of new technologies
- Ongoing Security Program
- Ongoing Asset Management Program
- Annual life cycle replacement of servers, PCs, laptops, printers
- Implement Electronic Personnel Folders (OPF)

To achieve this vision, NLRB will reallocate its information technology funds to those areas that directly support its strategic planning efforts. NLRB's IT budget will not significantly increase in 2007, but funds will be reallocated from the maintenance of legacy applications to new application development and implementation.

This redistribution of funds is directly tied to the Agency's transition from case tracking systems to an enterprisewide case management system. Funds allocated to Administrative Systems increase incrementally since these systems are outsourced to the Department of Interior's National Business Center (NBC).

The following sections present a detailed discussion on NLRB's major information technology initiatives. A strategic justification is provided for each investment, as well as its ability to support the strategic goals outlined in the President's Management Agenda.

4.1 Modernize Business Systems

Challenges Addressed	Other Strategies Supported
■ Increasing Customer Expectations ■ Costs of Maintaining Multiple Applications Built With Diverse Technologies ■ Federal IT Mandates and Initiatives	■ E-Government

4.1(a) *Replace Legacy Case Tracking Systems*

The NLRB will develop the integrated Next Generation Case Management (NGCM) to support case management, electronic case files, workflow, document management, and customer relationship management. The NGCM will support business units across the Agency. It will be composed of COTS applications customized to meet the business needs of the NLRB. Eventually, the NGCM will replace the core NLRB legacy business applications, including:

CATS
PCL
TIGER
LION
RAILS
ACTS
Special Litigation
EOTS

While the NGCM is being implemented, the NLRB will continue to maintain the existing case management applications supporting the Agency's business units, e.g., CATS, PCL, and TIGER. As a general rule, these applications will be maintained in a "break/fix" mode only. Change requests will be reviewed and approved as needed when the application is broken, or requires changes as a result of legislation. The applications will also receive the changes/corrections needed to maintain data integrity.

4.1(b) *Complete JCMS*

JCMS is an umbrella label for planning, developing, designing, implementing, documenting, and maintaining all computer applications used by the Offices of the Board Members, the Office of the Executive Secretary, the Office of the Solicitor, the Office of Representation Appeals, the Division of Information, and the Division of Judges (both Headquarters and Branch offices) of the National Labor Relations Board (NLRB). Currently, Board stage 3 processing is implemented using JCMS. Shortly, stages 1 and 2 will be implemented for the ES and Board member offices. In FY 2007, JCMS will be expanded into all the Board offices.

4.1(c) *Implement an E-Government Portal*

The NLRB will use the IRB process to identify and prioritize E-Government opportunities. These areas will then be targeted for E-Government pilot projects that will be accessible through the public-facing portal. This portal will be built implementing features that include:

- Data collection
- On-line case status
- End user personalization and customization
- Historical records/documents research
- E-Filing

4.1(d) *Implement Enterprise Content Management*

The first phase of ECM will consist of establishing e-Rooms for all the Regional and HQ offices. The process will be manual at first (drag and drop documents into e-Room), however, as the E-Filing initiative takes effect, documents that come in from the public will be placed in the appropriate e-Room. The e-Rooms can then be shared between Regional and HQ offices as needed.

As the requirements for digital content grows, the Agency will look to standardize on an ECM package that supports all requirements needed today and 5–10 years into the future.

A key component and strategy this Agency will need to address is E-Discovery. Federal rules have been modified to force attorneys to acknowledge that E-Discovery issues exist in their cases very early in the case processing cycle. Additional proposed legislation constitutes an attempt to make courts aware of the need to address electronic data in the pretrial conference stage, acknowledge existence of electronic data early in the case processing cycle, and avoid excessive discovery costs. OCIO understands the need to support the activities the Agency will undertake to implement policies and procedures surrounding E-Discovery. The timing, storage, disposal, and accessibility of electronic data will serve as key factors in the Agency's decisions regarding what guidelines and procedures will exist for E-Discovery.

As E-Discovery evolves, other content will need to be brought into the mix to include e-mails, web pages, and other unstructured content stored on network file servers.

4.2 Enhance Enterprisewide Planning

Challenges Addressed	Other Strategies Supported
▪ Rapidly Changing Technology ▪ Increasing Customer Expectations ▪ Federal IT Mandates and Initiative ▪ IT Budget	▪ Implement Formalized Enterprise-Wide Planning ▪ Modernize Business Systems ▪ Provide A Secure And Robust It Environment

4.2(a) *Enterprise Architecture*

The NLRB is building an Enterprise Architecture management foundation by increasing the Agency's level of Enterprise Architecture awareness, describing the As-Is and the eventual To-Be architectures, and developing the implementation plan for the Agency to achieve its desired Enterprise Architecture direction.

NLRB's Enterprise Architecture plans follow the guidance provided by the Federal CIO Council. Management understanding and participation is a key success factor for Enterprise Architecture and the IT Capital Planning and Investment Control process at NLRB.

4.2(b) *Capital Planning*

The NLRB recently formalized a CPIC process, created the Investment Review Board and an Executive Steering Committee to guide all IT planning for NLRB, helping to build a sound portfolio of IT investments for the Agency. The new CPIC process will use the Enterprise Architecture and the Information Technology Strategic Plan (ITSP) as tools in identifying and prioritizing opportunities for major business process reengineering, systems development, and E-Government initiatives.

4.2(c) *IT Strategic Plan*

The OCIO will continue to apply the most effective and proven best practices while developing the IT Strategic Plan. Building a comprehensive IT Strategic Plan that aligns with the Agency's business strategy is essential to ensuring NLRB success. The OCIO will invest in tools such as templates, learning guides, and other resources such as Gartner Research to stay up to speed on the latest issues concerning IT strategy and governance. These technologies will also enable the timely preparation, update, approval, and deployment of the NLRB IT Strategic Plan.

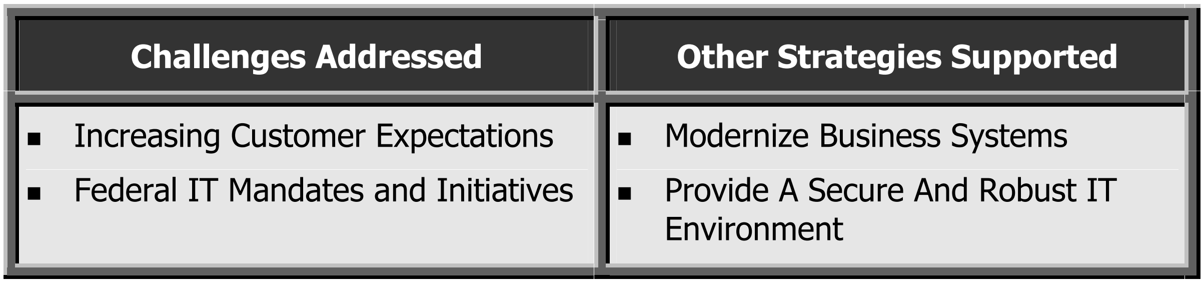
4.2(d) *Program Management Office*

In FY 2005, the Office of the CIO was reorganized to focus on business and IT alignment and to put more emphasis on project management. With the approval of Chairman Battista, the OCIO created a Program Management Office to more effectively manage the multitude of projects in the OCIO project portfolio.

In March 2006, the OCIO hired an Associate CIO for the Program Management Office. The goal of the PMO is to provide the strategic direction for IT within the NLRB. Its FY06 objectives are the following:

- Implement Primavera Portfolio/Project management software
- Train OCIO staff in Project Management
- Develop PM templates for the OCIO staff to use
- Manage the biweekly communications of project and task status
- Manage the Investment Review Process
- Maintain the Enterprise Architecture
- Maintain the IT Strategic Plan
- Develop and implement IT acquisition strategies

4.3 Provide a Secure and Robust IT Environment



Challenges Addressed	Other Strategies Supported
▪ Increasing Customer Expectations ▪ Federal IT Mandates and Initiatives	▪ Modernize Business Systems ▪ Provide A Secure And Robust IT Environment

4.3(a) *Infrastructure Modernization*

4.3(a)(1) *Server Hosting*

The National Labor Relation Board (NLRB) will outsource the management of its data servers to a secured and environmentally hardened Data Center owned by a vendor. The Data Center will host applications and servers that perform services such as File/Print Services, Internet Website Services, Intranet Website Services, Database Services, Email and Calendaring Services, and Remote Access Services within the Data Center. The Agency is taking a phased approach to move all of it servers to two data centers located on the east and west coasts.

4.3(a)(2) *Hardware Consolidation and Centralization*

The National Labor Relations Board (NLRB) is in the process of consolidating our IT resources into two collocated facilities. The collocation facilities will be located on the east and west coasts. The first phase of the consolidation effort will be consolidating the file and print services. NLRB currently uses Novell Netware for file and print service.

There are 56 Novell Netware servers located in the Agency's 52 field offices and the Headquarters office in Washington, DC. We will replace all Novell servers with Network Area Storage (NAS) devices located on the east and west coast at two co-locations facilities. The NAS will be configured to allow for replication between the two sites and provide disk to disk to tape backup as the backup solution for the storage devices. NLRB has an estimated 2200 users that will be affected by the consolidation effort. The NLRB will stop using Netware as it network operating system once the file and print service consolidation is completed. All servers will be Windows 2003 and use Active Directory for authentication. The Agency will also consolidate its six e-mail servers and move this service into the east and west coast data center.

4.3(a)(3) *Content Addressable Storage*

Internal efficiency and effectiveness is of utmost importance to the NLRB especially as it becomes more citizen-centric. Making data available anytime, anywhere will require the Agency to take a look at its file system to answer the question of whether or not it is better to continue with a traditional file system approach (record the location of where data are stored) versus using a content addressable storage solution (a mechanism for storing information that can be retrieved based on it's content, not its storage location). Content-addressed storage systems have emerged to help IT managers protect business data while keeping it accessible and searchable.

As part of its technical architecture "to-be" the NLRB will evaluate digital asset management as a tool to manage its data storage and retrieval processes.

4.3(a)(4) *Wireless Technology*

Currently, the network switches at NLRB HQs are over 7 years old, beyond the end of their lifecycle and not IPv6 compliant. Due to the investment involved, the OCIO is going to evaluate wireless technology. It's possible that the end solution may be a combination of wired devices (between floors, core switch, and switch to server) and wireless access points on the floors.

The OCIO will also expand its use of wireless network technology (in a limited mode) to conference rooms within the NLRB to facilitate approved vendor demos and presentations through a secure wireless connection into the network.

4.3(a)(5) *Network Convergence and IPv6*

Network convergence provides a standard platform designed to allow easy integration of e-mail, voice, fax, and other telephony applications, thereby consolidating network administration enterprisewide. Vendors are positioning to take a holistic view of the evolution and implementation of next generation unified networks for voice, data, and video services. During FY 2007, OCIO will continue to monitor industry progress in this area so that a determination can be made for when the technological solutions have matured and the agency is ready to move forward with network convergence.

During FY 2008, the OCIO will evaluate the feasibility of establishing an NLRB private wide area network instead of the public VPN WAN contracted through MCI. By establishing a private network, the NLRB will have more control over bandwidth issues, security and quality of service (QOS). QOS is essential for latency sensitive applications such as VoIP and Video Teleconferencing (VTC).

4.3(a)(6) *Project Management and Performance Tracking*

The current project management responsibility resides with the Chief for Information Infrastructure, however, all program managers meet weekly with the CIO and Deputy CIO to review the status of all projects and verify that current results, resources, and approaches are still on schedule and are consistent with current IT operations.

4.3(b) *FISMA*

In support of FISMA, the IT staff has conducted several reviews, audits, and assessments of the IT Security Program. In addition, OMB performed an assessment of the Program, which was conducted in accordance with the Special Publication (SP) 800-26 and the Federal IT Security Assessment Framework produced by the National Institute of Standards and Technology (NIST). The Federal IT Security Assessment Framework and 800-26 identify profile levels associated with an IT Security program.

The NLRB IT Security plan has four specific functions: Guidance, Adherence, Compliance, and Maintenance of approved IT security practices. This plan includes the development of an IT Security program focusing on the following:

4.3(b)(1) *IT Security Program Update*

NLRB has developed Policies, Guidelines & Standards; a Computer Incident Response Team (CIRT); and continuously researches applicable new IT Security Technology. NLRB's Security Officer oversees the development of all IT Security policies created in-house or with the support of contractual services to ensure that all pertinent policies are developed in accordance with applicable laws and regulations.

4.3(b)(2) *IT Security and Awareness*

In accordance with OMB Circular A-130, the IT Security Awareness and Training Program develops an NLRB-wide security awareness, training, and education program plan to deliver and implement solutions for delivering computer-based training (CBT) to Agency employees. NLRB employs a variety of security training mechanisms including CBT courses, conferences, formal classroom training, and seminars.

4.3(b)(3) *IT Certification and Accreditation*

NLRB will continue to address all Federal (including OMB) and NLRB requirements regarding an IT system prior to the system entering its operations phase. The C&A process ensures appropriate security has been incorporated into each system by identifying risks, implementing measures to mitigate those risks, and planning for business continuity in cases where those risks impact operations. NLRB will then obtain management approval to operate with residual risks.

4.3(b)(4) *IT Vulnerability Testing and Correction*

NLRB conducts compliance reviews to validate that the security roles and responsibilities for oversight and management of all IT security issues such as remote access; firewalls; network and application authentication; virus detection & protection; and intrusion detection are followed in accordance with properly documented procedures. Specific activities include visiting Regional sites, running audit logs of users to validate user access, and running password cracking semiannually.

4.3(b)(5) *Contingency Planning*

NLRB will develop a Disaster Recovery (DR) plan to assure that mission-critical systems are identified as priorities. NLRB's DR will describe the appropriate response to any situation that may jeopardize the integrity, availability, or confidentiality of data, data processing, or telecommunications facilities.

4.3(b)(6) *Homeland Security Presidential Directive-12 (HSPD-12)*

NLRB will develop a plan for the implementation of a secure and reliable form of identification for agency employees. HSPD 12 is directed towards enhancing security, increasing government efficiency, reducing identify fraud, and protecting personal privacy by establishing a mandatory, Governmentwide standard for secure and reliable forms of identification.

4.3(b)(7) *Program management and Performance Tracking*

There are several IT Security initiatives that comprise the IT Security Program. These initiatives require support services and may call for additional hardware products. The acquisition strategy is to use contracting support wherever and whenever available. As mentioned previously, the IT Security Program currently consists of one Federal employee responsible for managing all of the IT Security Program initiatives, including the CIRT program which will be contracted out to provide services 24 hours a day, 7 days a week.

4.4 Maintain Currency with IT Best Practices

Challenges Addressed	Other Strategies Supported
▪ Rapidly Changing Technology ▪ Increasing Customer Expectations ▪ Change Management	▪ Enhance Enterprisewide Planning

4.4(a) *Information Technology Infrastructure Library (ITIL)*

In 2005, the OCIO assigned a Project Manager full time for the implementation of ITIL. To date, a formal change management process has been setup. A Change Advisory

Board (CAB) has been organized that effectively approves all requests for change (RFC). The OCIO has adopted the language used by the ITIL framework and maintains all documentation in EMC collaboration tool, E-Room.

The OCIO helpdesk is fully staffed and managed by a contractor. The OCIO uses HEAT to track customer calls and provide problem resolution. Customer service surveys are sent out after each ticket is completed. The customer service satisfaction level is greater than 95 percent per month on average.

The OCIO has had an Asset Management program in place for some time now and has an individual whose fulltime job and responsibility is Asset Management.

In FY 2007, it is the OCIO goal to move beyond change management and implement the second important control process within the ITIL framework, Configuration Management. Change management, Asset Management and Configuration Management are considered “primary controls.”

4.4(b) *Life Cycle Management*

OCIO will continue to budget for the annual refresh of personal computers, systematic replacement of network servers, software maintenance, and other peripheral devices to include printers, PDA’s, scanners, and other mass storage devices.

4.4(c) *Open Standards*

OCIO will continue to use open standards when delivering IT solutions within the Agency.

4.5 Appendix A—Glossary

GPRA—The Government Performance and Results Act (GPRA) of 1993 establishes performance reporting as part of an integrated planning, budgeting, management, and performance assessment system. GPRA emphasizes improved service delivery by requiring agencies to focus on results, service quality, and customer satisfaction. The Act both requires and encourages consultation with customers and Congress to gather customer and stakeholder feedback, input, and insight for the development of strategic and performance plans.

ITMRA—The Information Technology Management Reform Act of 1996 (ITMRA)—referred to as the Clinger-Cohen Act provides for the integration of the information technology management process with the processes for making budget, financial, and program management decisions. ITMRA encourages incremental acquisition of information technology systems as well as the acquisition of Commercial-Off-The-Shelf information technology products. The Act also requires the consideration of information technology goals in strategic planning as well as information technology contributions to Agency goals and performance.

Information Technology Investment Guidance—On October 25, 1996, the Office of Management and Budget issued guidance (referred to as the "Raines Rules") to agencies on how to manage information technology investments in keeping with the provisions of the GPRA and Clinger-Cohen Act.

Information Technology Architecture—On June 18, 1997, the Office of Management and Budget issued guidance (M-97-16) to agencies on the development and implementation of Information Technology Architectures. This Information Technology Architecture describes the relationships among the work the agency does, the information the agency uses, and the information technology that the agency needs. The architecture also includes standards that guide the design of new systems.

Capital Programming Guide, version 1.0 In July 1997, the Office of Management and Budget issued guidance to supplemental circular A-11, part 3. This guide provides a process for portfolio analysis, risk management, planning, performance management, budgeting, and other related activities.

GPEA—The Government Paperwork Elimination Act (GPEA) of 1999 requires agencies to implement the capability of optional electronic interactions for all transactions by October 2003. The Act also requires agency acceptance of electronic signature for these transactions when conducted with 50,000 or more customers.

FISMA—The Federal Information Security Management Act (FISMA) requires that agencies submit reports to OMB based on annual assessments identifying security gaps both within and across agencies.

4.6 Appendix B—Acronym

ACTS=	Appeals Case Tracking System
AIIM=	Association of Imaging and Information Management
ANSI=	American National Standards Institute
C&A=	Certification and Accreditation
CAB=	Change Advisory Board
CATS=	Case Activity Tracking System
CBT=	Computer-based Training
CIRT=	Computer Incident Response Team
COTS=	Commercial Off-the-Shelf
CPIC=	Capitol Planning and Investment Control
DR=	Disaster Recovery
ECM=	Enterprise Content Management
EOTS=	Extension of Time System
FISMA=	Federal Information Security Management Act
FOIA=	Freedom of Information Act
G2C=	Government to Citizen
GPEA=	Government Paperwork Elimination Act of 1999
GPRA=	Government Performance Results Act of 1993
GPS=	Global Positioning System
HEAT=	Helpdesk Expert Automation Tool
HSPD-12=	Homeland Security Presidential Directive-12
IETF=	Internet Engineering Task Force
IETF=	Internet Engineering Task Force
IP=	Internet Protocol
IPT=	Integrated Project Teams
IPv6=	Internet Protocol Version 6
IRB=	Investment Review Board
ISO=	International Organization for Standardization
ITIL=	Information Technology Infrastructure Library
ITMRA=	Information Technology Management Reform Act
ITSP=	Information Technology Strategy Plan
JCMS=	Judicial Case Management System
LION=	Litigation Information on the Network
MBDD=	Microsoft Business Desktop Deployment
NBC=	National Business Center
NGCM=	Next Generation Case Management
NIST=	National Institute of Standards and Technology
NSA=	Network Area Storage
PCL=	Pending Cases List
PDA=	Personal Digital Assistant
PDAs=	Personal Digital Assistants
PMA=	President's Management Agenda
PMO=	Program Management Office
RAILS=	Regional Advice Injunction Litigation System
RFC=	Requests for Change
SBU=	Sensitive But Unclassified
SOA=	Service Oriented Architecture

SP=	Special Publication
SQL=	Structured Query Language
TCP=	Transmission Control Protocol
TIGER=	Trial Information Gathered on Electronic Records
VP=	Virtual Processor
VTC=	Video TeleConference
W3C=	World Wide Web Consortium
WAN=	Wide-Area Network
WWANs=	Wireless Wide-Area Networks