

APPENDIX Q — Enabling Strategies

The transformation of the Postal Service now underway necessarily involves a restructuring of functional activities that facilitate and enable the work of the organization. Financial management must be enhanced to improve financial reporting transparency and the ability of the Postal Service to finance capital improvements. Further development of the Information Platform and better use of technology are essential to support modernization in all areas. Securing the mail, the mission of the Postal Inspection Service, has never been more important. Regulatory reforms, likewise, must be pursued to support the Postal Service to respond to transformational imperatives.

This Appendix to the *Transformation Plan* contains additional explanation, detail, and examples of near-term strategies that enable the organization. This is not meant to be a comprehensive list of postal projects, but meant to outline those that will contribute to the success of postal transformation.

Strategies in this Appendix include:

- Enhance Financial Management;
 - Debt Management
 - Monthly Reporting
- Expand Usage of Supply Chain Management;
- Strategically Apply Technology; and
 - Enhanced Security
 - Upgraded Infrastructure
 - Universal Computing Connectivity
- Ensure Safety and Security of the Mail, Customers, and Employees.

Debt Management

Overarching Objective

Reduce outstanding debt

Strategy: Reduce debt and remain within the current statutory debt limits

By recovering prior year losses and maintaining a disciplined capital investment program, the Postal Service will endeavor to limit financial risks by reducing debt and remaining within the \$15 billion debt limit.

Substrategy: Preserve liquidity while managing interest expense

The plan to remain within the \$15 billion debt limit will be modified as necessary to ensure that the Postal Service preserves its ability to meet all of its cash obligations. The Postal Service will continue to adjust the amount of floating-rate and fixed-rate debt to manage interest expense and mitigate the risks posed by higher interest rates.

Background

Under current law the Postal Service may increase its outstanding borrowing by up to \$3 billion annually, which includes a \$2 billion increase for capital investments and a \$1 billion increase for operating expenses. The Postal Service is subject, however, to a total debt limit of \$15 billion, which has been in place since 1992, when it was raised from \$12.5 billion. Prior to 1991, the debt limit had remained at \$10 billion since postal reorganization. The law also requires the Postal Service to notify the Secretary of the Treasury at least fifteen days prior to offering debt obligations. The Secretary has a right of first refusal to purchase the Postal Service debt within the fifteen-day period or a commercially reasonable time period thereafter. Since 1974, the Postal Service has borrowed exclusively through the Treasury's Federal Financing Bank. In the past several years, the Postal Service and the Treasury have reached agreement on important issues related to borrowing. As a result, the Postal Service currently has the flexibility required to manage its debt.

Debt is a reflection of capital spending and overall financial performance. Over time, changes in debt are largely determined by the difference between cash flow from operations and capital outlays. Cash flow from operations is influenced by net income (or losses), and noncash expenses such as depreciation. Capital cash outlays are the funds invested in capital improvements such as facilities, automation equipment, and information technology. From 1997 through 2001, Postal Service capital cash outlays exceeded cash flow from operations by \$5.2 billion. Consequently, debt increased by \$5.4 billion—from \$5.9 billion to \$11.3 billion—during that time. Cash on hand at the end of fiscal year 2001 totaled approximately \$1 billion, or less than one payroll.

The Postal Service has managed its mix of short- and long-term debt to lower its interest expense over time. As a result of this strategy and lower interest rates, annual interest expense on Postal Service debt remains lower than it was during much of the 1990s. Current interest expense is but one of the potential costs associated with debt. However, the fact is that Postal Service debt—the obligations that are subject to

interest and principal payments—almost doubled between the ends of fiscal years 1997 and 2001, from \$5.9 billion to \$11.3 billion. While interest rates may or may not remain relatively low, a more important consideration is that the increase in debt, however necessary to preserve liquidity, has also increased financial risk by adding to the obligations of the Postal Service. In light of risks to mail volume growth, which create risks to cash flow, the Postal Service’s capacity to service growing debt is limited.

The Postal Service has attempted to determine an appropriate debt level. The Postal Service has considered various means of evaluating its debt ceiling, including post-1992 revenue growth, asset growth, and inflation. Such analysis has major drawbacks, however, because it assumes that the debt ceiling of \$15 billion was optimal when instituted in 1992; and the analysis does not assess the future risks facing the Postal Service. By remaining within its \$15 billion debt limit, the Postal Service can limit the risks it carries into administrative and legislative transformation.

As mentioned earlier, the change in debt is largely determined by the difference between cash flow from operations and capital cash outlays. Since cash flow from operations is linked to net incomes (losses), stabilizing and reducing debt will require that the Postal Service recover its prior year losses and carefully plan its capital cash outlays so they do not exceed cash flow. As the past two fiscal years have demonstrated, the Postal Service cannot simultaneously generate net losses and reduce its borrowings.

As a final point, the consequences of running out of cash far exceed the costs of increasing debt. Therefore, the Postal Service will do what is necessary to keep from running out of cash, even if doing so means accepting a temporary increase in its statutory debt limit. Under such an outcome, the Postal Service would seek to reverse the temporary increase in debt, and resume its strategy of keeping its debt below \$15 billion, while reducing outstanding debt.

By reducing outstanding debt, by remaining within its \$15 billion debt limit, and by managing its interest expense, the Postal Service can limit the risks it carries into administrative and legislative transformation.

Metrics

Amount of debt and interest expense

Interdependencies

The Postal Service’s ability to apply cash flow toward debt reduction requires both recovery of prior year losses and some limits on capital investments.

Monthly Reporting

Strategy: Convert Postal Service reporting (financial and all other) from the existing accounting period format to a calendar month format

Background

The Postal Service, for financial reporting purposes, uses both a postal fiscal year (PFY) and a government fiscal year (GFY). The Postal Fiscal Year is used for internal reporting and the Government Fiscal Year is used for rate cases and reporting annual audited financial statements.

The Postal Fiscal Year consists of thirteen, four-week accounting periods. Each accounting period consists of two biweekly payroll cycles. The Postal Service assumes that the construction of the thirteen accounting period fiscal year was mandated by the need for accurate reporting of salaries and benefits that constitute approximately 75 percent of Postal Service total costs. This could only be accomplished by including complete payroll cycles. Up until the implementation of the new Time and Attendance Control System (TACS) no daily information was available as part of Postal Service timekeeping systems.

A postal quarter (PQ) consists of three consecutive accounting periods except for PQ 4, which consists of the last four accounting periods of the fiscal year.

Trends / Supporting Data

One of the major disadvantages inherent in the present structure is that the Postal Fiscal Year is only 364 days long. The Postal Service does not add the extra day (or two) to align the PFY to the calendar year because of the necessary tie to the payroll cycle. That means that every five or six years, the PFY slips by one week, making the PFY more and more out of line with the GFY. For example, the end of PFY 2001 was September 7, 2001. The end of the GFY was September 30, 2001. The start of PFY 2001 was September 9, 2000. The start of GFY 2001 was October 1, 2000. Normally this difference does not result in major changes because the two periods (at the start of the PFY and at the end of the GFY) are similar. However, this year, the period at the end of the GFY (September 8-30, 2001) was eventful.

The Postal Service reports year-to-date performance as if the fiscal year started with the PFY, starting with accounting period (AP) 1 reports, AP 2 reports, etc. It is not until the end of the GFY that the year to date reporting is realigned with the GFY. This is somewhat problematic for FY 2002, because of the events of September 11, 2001. The Postal Service reported much of the lost revenue, as a result of the terrorist attacks, in GFY 2001. However, the Postal Service continues to report the lost revenue in FY 2002 as AP 1 began September 8, 2001, before the attacks took place. This is somewhat confusing within the Postal Service and certainly more confusing outside the Postal Service.

Accounting period reporting is not unknown in private industry, but monthly reporting is far more common. Much of the data about the economy from state and federal government agencies and forecasts from governmental, commercial, and educational sources are reported in a monthly format. In addition most of private industry invoices, pays and mails on a monthly cycle. Most Postal Service customers and also Postal Service competitors report in a monthly format.

Monthly reporting offers the following advantages:

- Eliminates the need for the AP 14 reconciliation that occurs at the end of each GFY. This should facilitate the year-end close.
- Eliminates the Postal Fiscal Year. The Government Fiscal Year will be used for both internal and external reporting, for both Headquarters and Field reporting.
- Aligns the Postal Service with the vast majority of corporate reporting, with external databases and with governmental reports on economic data and with standard forecasts of economic activities. Therefore, it will provide the Postal Service financial data on a basis that enables comparative analysis with competitors, as well as consistency in current external reporting of financial results.
- Generates a small saving as the books will have to close only twelve times per year instead of fourteen. It should speed finalization of the audited end of year results.
- Should simplify the estimation of accruals at the end of the fiscal year.
- Should make certain expense and revenue data more stable when reported on a monthly basis. Most private sector companies invoice and pay on a monthly basis. The end of the month burst in transactional activities will occur consistently every reporting period.
- Eliminates confusion that is created by the use of two reporting systems.
- Facilitates conversion to any alternate fiscal year.

Substrategy: Monthly Reporting — Converting from accounting period reporting to monthly and calendar quarter reporting

There are many different ways in which the Postal Service can convert to monthly reporting. At this stage, things are still flexible. Generally, the Postal Service sees no reason to change its bi-weekly payroll cycle. Payroll expenses will be mapped into months based on the percentage of hours used in each month for any pay period that overlaps two months.

Weekly reporting (from a Saturday to Friday format) will continue for many systems. The AP-to-date reporting will be replaced with month-to-date reporting.

The Postal Service's general strategy will be to put interim systems in place by the start of FY 2003 to allow us to crosswalk accounting period reporting into monthly reporting. Starting with FY 2004 Postal Service systems should be fully converted.

Metrics

Frequency of reporting

Timeline

- Identify systems that need to be modified for monthly reporting (Corporate wide) (Jan 2002 – Mar 2002).
- Create strategies for interim reporting in FY 2003 (April 2002 – May 2002).
- Implement those strategies (June 2002 – Aug 2002).
- Create permanent solutions for monthly reporting (Sept 2002 – March 2003).
- Test the permanent solutions by preparing pro forma monthly reports for June, July and August (April 2003 – June 2003).
- Fully implement monthly reporting (Sept 2003).

Interdependencies

This strategy lies entirely within the control of the Postal Service. Currently, there are no conflicts with required government reporting.

Supply Chain Management

Overarching Objective

Continue to implement and institutionalize supply chain management. Supply chain management is the analysis of the purchase process and the supply stream, from the supplier's supplier to the customer's use and disposal, in order to increase customer satisfaction and decrease overall cost. Effective supply chain management involves a number of business practices, including close interaction among end users, buyers and suppliers, long-term contracts, and ongoing analysis and improvement of operating and administrative processes. Its institutionalization, in terms of business practices, organizational design and deployment, and supplier relations, will lower overall costs and improve customer service.

Strategy: Focus Postal Service resources on lowering overall cost and furthering competitive and business objectives

Substrategy: Consolidate purchases for better quality and lower cost

Redesign purchasing organization into interdisciplinary commodity teams. Reduce low-dollar value transactions and forge stronger and more effective relations with key, strategic suppliers.

Background

The Postal Service awards contracts worth billions of dollars every year. Supply chain management maximizes these expenditures, and brings them to bear on the marketplace. Over the past several years, supply chain management has become one of the most successful aspects of contemporary businesses, and it is becoming increasingly so for the Postal Service. Process and demand management, data analysis, and other business practices provide cross-functional purchase teams with the tools to focus on strategic sourcing, while low-dollar value—but administratively expensive—transactions are minimized. Innovative business practices, such as reverse auctioning and Internet technologies like Web-based ordering are also being used to

good effect. The purchasing and material management functions are being redesigned and redeployed to take advantage of varied business expertise through the use of multidisciplinary teams. Results to date have been impressive: in FY 2001, cost reductions had been predicted to be \$100 million, but actually reached \$157 million. Greater cost reductions will be achieved in FY 2002.

Interdependencies

Communication and cooperation between and among internal Postal Service customers, buyers, and suppliers is essential to long-term success. In addition, supply chain management is a cross-disciplinary business philosophy, and requires expertise in logistics, purchasing, contract pricing, commodities and other areas in order to be truly effective. Purchasing and Materials is redesigning its organization to best deploy these skills.

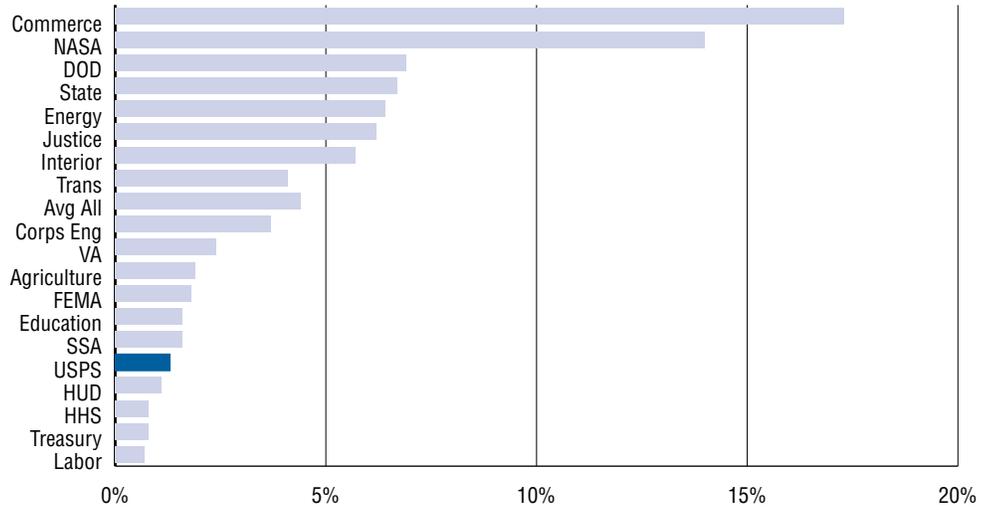
Obstacles

As supply chain management becomes more and more prevalent in Postal Service purchasing and supplying activities, resistance can be expected from some segments of the supplier community, especially as the supplier base shrinks. Certain statutory requirements, such as the Service Contract Act and the Davis-Bacon Act, also add cost and administrative efforts with which commercial businesses are not burdened. Overcoming such obstacles would require the revision of a number of federal statutes, or alternatively, the postal enterprise should be summarily exempted from such statutes.

Strategic Application of Technology

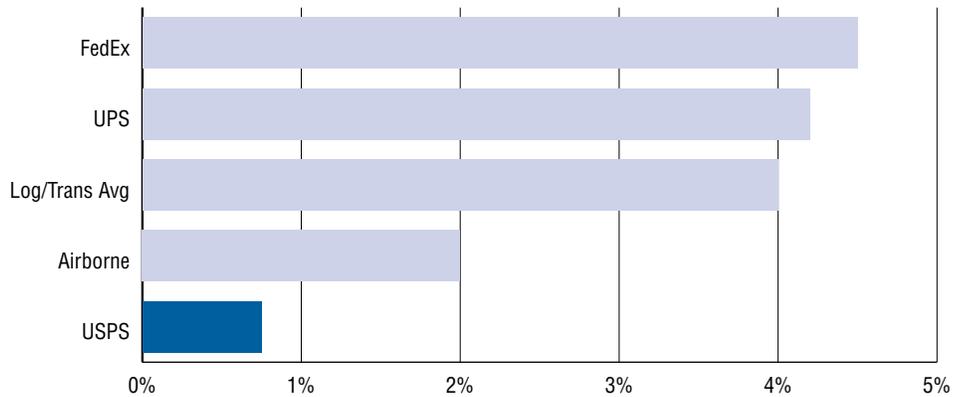
The Postal Service invests a significantly smaller percentage of its total budget in information technology than any other federal agency (see Figure 1) and private sector competitor (see Figure 2).

FIGURE 1: FEDERAL AGENCY COMPARISON — INFORMATION TECHNOLOGY BUDGET AS A PERCENT OF THE TOTAL BUDGET



Source: Office of Management and Budget, Clinger Cohen Act Report on Fiscal Year 2002 Federal Information Technology (IT) Investments, April 19, 2001; Postal Service forecast data for Fiscal Year 2003.

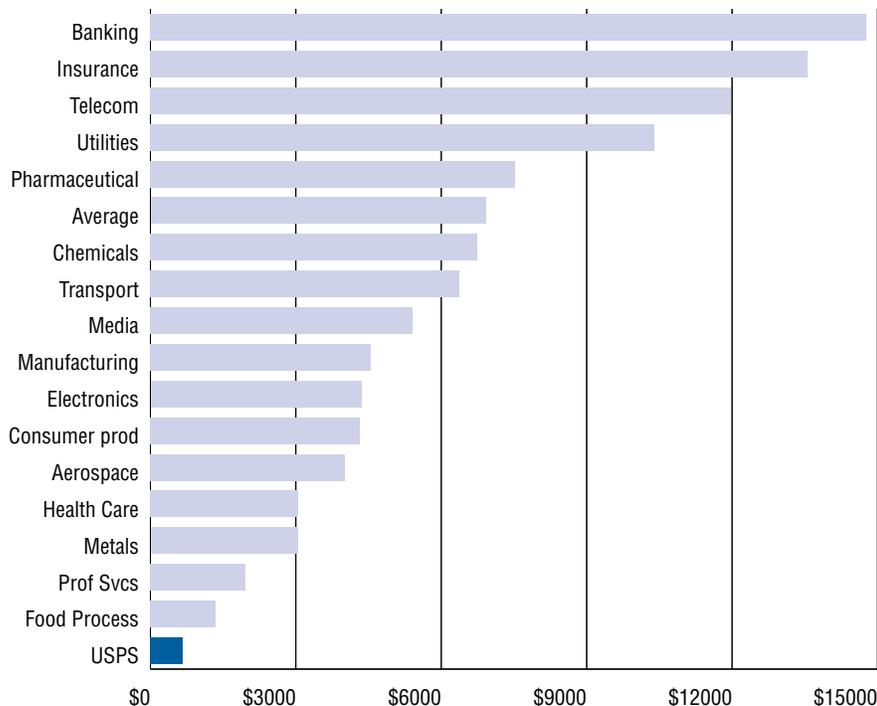
FIGURE 2: PRIVATE INDUSTRY COMPARISON — INFORMATION TECHNOLOGY BUDGET EXPRESSED AS A PERCENTAGE OF REVENUE



Source: 10-K filings, InfoWeek 500 analysis, Postal Service data.

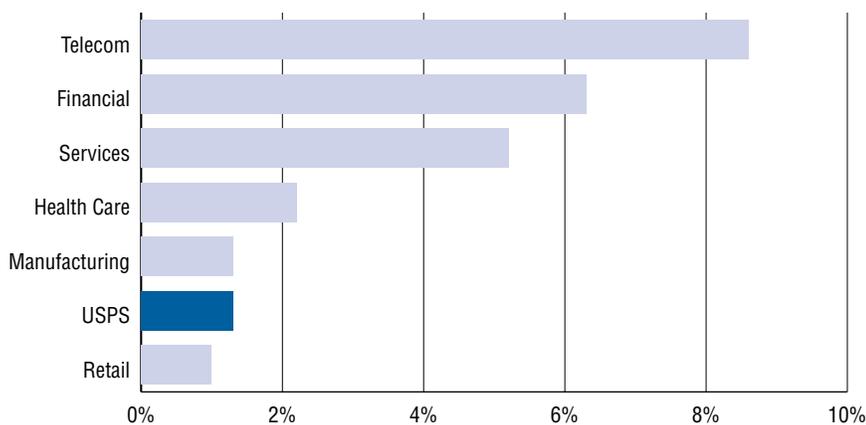
In comparison with other industries, the Postal Service’s investment in information technology per employee (see Figure 3) is the lowest of all. Expressed as a percent of an organization’s total budget, the Postal Service’s investment in information technology is also the lowest (see Figure 4).

FIGURE 3: PRIVATE INDUSTRY COMPARISON — INFORMATION TECHNOLOGY BUDGET EXPRESSED AS AN AVERAGE INVESTMENT PER EMPLOYEE PER INDUSTRY



Industry Average Source: Information Week survey data (1997). Postal Service data: Total CTO Budget (including customer IT budgets) divided by the number of employees.

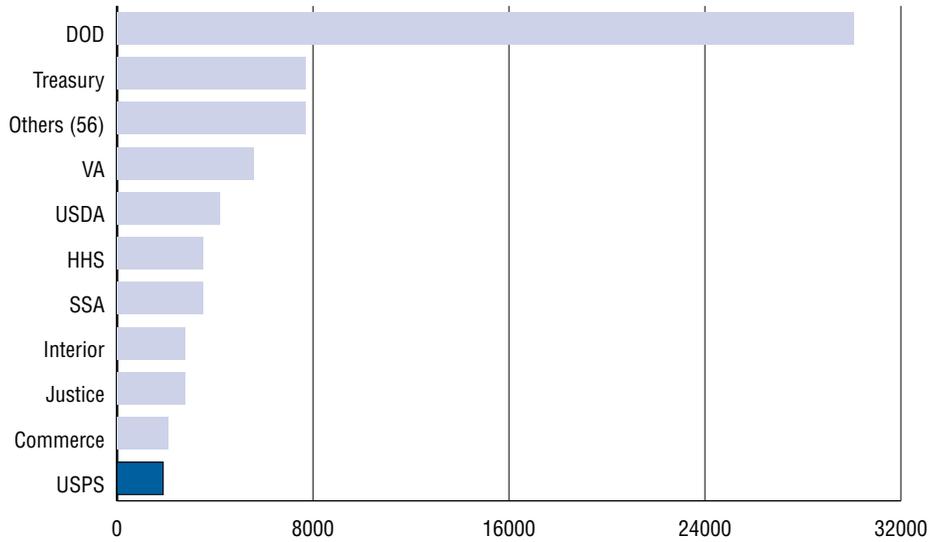
FIGURE 4: PRIVATE INDUSTRY COMPARISON — PERCENT OF BUDGET ALLOCATED TO INFORMATION TECHNOLOGY BY INDUSTRY AVERAGE



Industry Average Source: Information Week survey data (1997). Postal Service data: Total CTO Budget (including customer IT budgets) divided by \$65 billion.

The number of information technology resources in comparison with federal agencies (see Figure 5) is the lowest of all.

FIGURE 5: FEDERAL AGENCY COMPARISON — THE NUMBER OF FEDERAL EMPLOYEES BY DEPARTMENT



Source: Office of Personnel Management, Federal Workforce Statistics. Total Number of GS 332, 334, 335, and 340, (approx. 70,000) verified by IT Workforce presentation, divided by the percent of GS 334s identified by agency. GS 334s represent 80 percent of Federal IT workforce.

The clear message in these comparisons of investment and resources is that the Postal Service manages its information technology functions efficiently and effectively with limited resources. This is accomplished via prudent spending, excellent management practices, and a dedicated workforce committed to the Postal Service's success.

Enhance Security Across All Technology

Overarching Objective

Managed by the Information Security Executive Council, which is composed of the Postal Service executive leadership and chaired by the Deputy Postmaster General, the Corporate Information Security Office implements prudent enterprise wide security strategies across the enterprise. The strategy aims to protect data entrusted to the Postal Service by contractors, business partners, and customers; to ensure the continuity of its business infrastructure; and to preserve its vast investment in technologies and information. The approach to implementing this strategy is outlined in the Postal Service's *Information Security Five-Year Strategic Plan*.

Strategy: Enhance security across postal technologies to avoid disruptions in critical operations and protect sensitive information from unauthorized disclosure or modification

Substrategy 1: Education and training

Background

In November 2000, the Postal Service Board of Governors approved a three-year, multimillion dollar, enterprise wide enhanced security program. Managing the security program is primarily the responsibility of the Corporate Information Security Office, while managing the system certification and accreditation process and business continuity and contingency planning are the responsibility of the various business organizations and their respective portfolio managers. Key to the success of the information security strategy are the assurances that security policies and practices are enhanced, implemented, enforced and that the vision and mission of the Postal Service are supported.

Both government and industry experts agree that communication is an integral part of a successful implementation of an information security strategy. The Postal Service recognizes this and considers awareness and training to be one of the most cost-effective information security investments. This substrategy includes activities to effectively educate, train, and create awareness of information security requirements; to define roles and responsibilities; and to enhance understanding of security risk management.

Milestones

- Establish information security internal Web site and reading room (2002)
- Conduct annual Computer Security Day activities (Annually)
- Develop awareness articles and outreach events (Annually)
- Publish role-specific learning plans (2003)
- Deploy distance-learning capability (2005)

Metrics

- Number of articles in Postal Service publications
- Number of visits to Information Security Web site and online reading room
- Number of executives and employees viewing awareness videos
- Number of internal and external outreach events and number of outreach contacts
- Number of staff trained in information security processes
- Number of people who use distance-learning courseware

Interdependencies

Developments of new threats, vulnerabilities, and new business and government requirements that may alter the security information, including roles and responsibilities.

Substrategy 2: Certification process

Background

The Postal Service has over 1,500 computer applications that run the business, which are divided into ten business portfolios: Finance, Purchasing, Marketing / Sales, Human Resources, Enabling, eBusiness, International, Delivery / Retail, Network Operations, and Product Tracking. To implement a standard security certification and accreditation process will provide a level of assurance that appropriate information security controls and processes are being implemented for all information resources based on their value to the organization and their risks. This assurance is required because one uncertified, and possibly insecure, information resource could introduce vulnerabilities that could negatively affect the security of another information resource. Ensuring appropriate protections are built into technology applications and services is essential for protecting the trust and confidence of Postal Service employees and customers.

This strategic focus is comprised of all security activities needed to accomplish the objective of achieving an acceptable level of security for all new products, services, and applications, and ensuring that security is reevaluated in legacy systems. In order to accomplish this strategy, the Postal Service developed a risk-based and cost-effective Information Security Assessment (ISA) process that provides business owners with a structured methodology to classify information resources, to identify security requirements, and to make informed deployment decisions (see Figure 6).

FIGURE 6: INFORMATION SECURITY ASSURANCE PROCESS



Milestones

Each of the ten portfolios has discrete milestones to accomplish this substrategy. The dates for accomplishing the milestones below depend on the number of new applications and legacy applications in the portfolio.

- Inventory systems (2002 through 2006)
- Assess using BIA (2002 through 2006)
- Prioritize systems (2002 through 2006)
- Complete ISA (2002 through 2006)
- Approve for deployment (2002 through 2006)

Metrics

Number and percentage of all new systems and legacy systems completing the ISA process that have been certified and accredited and accepted for deployment according to plan.

Interdependencies

Development of new threats and vulnerabilities and advances in technology.

Substrategy 3: Contingency planning

Background

This substrategy encompasses all activities needed to sustain mission-critical business information resources and operations in emergencies as mandated by the Critical Infrastructure Protection Act. As a result of the terrorist attacks on September 11, 2001, the Postal Service recently focused its efforts on this substrategy and updated its recovery plans to incorporate Federal Emergency Management Administration (FEMA) guidelines for Continuity of Operations Planning (COOP) into all major policies that pertain to Information Technology facilities which support critical information resources within the Postal Service.

The objective of this substrategy is to assure the continuity of essential business functions and recovery from a wide range of potential emergencies or threats, such as the recent terrorist and anthrax attacks. To support this substrategy, the Postal Service developed templates to guide business owners in addressing requirements for system availability and to integrate individual system continuity and contingency plans into overall plans, such as Continuity of Operations Planning and Disaster Recovery Planning.

Milestones

- Identify all critical system by portfolio (2002 through 2004)
- Establish contingency plans (2003 through 2006)
- Test selected contingency plan (2003 through 2007)

Metrics

Number and percentage of all new applications and systems and legacy systems having continuity plans compliant with standards and guidelines.

Interdependencies

Development of new threats, advances in technology, and updates in business / government contingency guidelines.

Substrategy 4: Intrusion protection

Background

Protecting the Postal Service infrastructure is a key component of Postal Service security strategy. Through this substrategy, the Postal Service will implement enhanced intrusion detection software, perform periodic network vulnerability tests, and scan Postal Service networks to identify vulnerabilities. To protect sensitive and critical information from unauthorized access or use and to maintain system availability, the Postal Service is using a layered defense approach, enhancing the strength of its firewalls, and guarding the external perimeter of its network. This will enable the Postal Service to better protect its servers and applications from both external and internal threats.

Additionally, this substrategy includes activities to mitigate hardware and software vulnerabilities by implementing vendor-identified security patches, software, and hardware upgrades; and to increase access and authentication controls using sophisticated password protection and access management. The key to this substrategy is to increase its response capability by enhancing the Computer Incident Response Team (CIRT), enabling the team to identify, contain, and respond to security incidents, breaches, and penetration attempts more efficiently.

Milestones

- Deploy standard baseline hardening standards for multiple devices and operating systems (2003)
- Implement standards for new components and retrofitting legacy components (Annually)
- Develop a process to detect problems closer to origin (2003)
- Define and implement additional layers of security within the infrastructure (Annually)
- Enforce new password and access standards (Annually)
- Complete deployment and implementation of intrusion detection capability on servers (2002 through 2005)

Metrics

- Number of servers and devices compliant with security standards
- Number of users with acceptable passwords
- Number of additional sensors deployed for monitoring

- Lapsed time in identifying, containing, correcting security incidents
- Number of attacks prevented from spreading through the layered defense
- Number of external attacks, viruses, and harmful e-mails prevented

Interdependencies

Development of new threats and advances in technology.

Substrategy 5: Automated monitoring

Background

To update its policies and procedures, the Postal Service reviewed vulnerabilities identified through third-party security experts, the Office of the Inspector General (OIG), and the General Accounting Office (GAO). Compliance with security policies requires an ongoing cooperative effort among several parts of the Postal Service, including the Corporate Information Security Office, the Chief Privacy Officer, the Office of the Inspector General, and the Computer Incident Response Team (CIRT). Additionally, the Postal Service coordinates with external organizations, such as the Federal Computer Emergency Response Team (FedCERT); the National Institute of Standards and Technology (NIST); the Systems Administration, Networking and Security (SANS) Institute; and other federal and industry experts, to ensure that the Postal Service is aware of emerging threats, vulnerabilities, mitigation approaches, and vendor patches.

The information security strategy will only be effective if individuals responsible for implementing policy, process, standards, and technology controls implement and maintain up-to-date practices. This substrategy includes activities to monitor compliance with policies to ensure that the Postal Service's technology environment achieves and maintains the desired level of security. The Postal Service will monitor user activities such as the acceptable use of e-mail, the Internet, and copyrighted software; network traffic; application and data access; computer intrusions; and other common threats and vulnerabilities.

Milestones

- Draft and publish compliance operating procedures (2002 through 2003)
- Produce reports that contain metrics for monitoring, review, and audit activities (Ongoing)
- Conduct periodic network scans with automated tools (Ongoing)
- Manually spot-check policy and process compliances (Ongoing)

Metrics

- Number of initial and repeat audit findings
- Number of successful penetration attempts
- Number of policy violations identified

Interdependencies

Development of new threats and advances in technology

Upgrade the Infrastructure

Overarching Objective

The Postal Service must continually upgrade and reengineer the computing infrastructure to support current and new business requirements. Improvements in the technology infrastructure are essential if the Postal Service is to become more efficient and reduce operating costs. The postal computing environment involves three tiers of computing: distributed, mainframe, and midrange. Each of these environments must be managed as separate upgrades, but all three efforts must be tightly integrated to provide seamless computing across the enterprise.

The upgraded infrastructure supports improvements in internal computing as well as enhancements to internal service offerings. These services leverage the improved infrastructure to expand its line of standardized technology solutions and automated administrative functions. The first service-focused strategy, technical shared services, provides mechanisms to build integrated rather than stove-piped applications. The second service-focused strategy, corporate shared services, utilizes the upgraded infrastructure to reengineer back-office functions, such as finance and human resources, across the enterprise.

Strategy: Leverage technological advances and business partnerships to upgrade and leverage the infrastructure

Substrategy 1: Upgraded distributed computing infrastructure

Background

Distributing innovative technology within the organization has enabled the Postal Service to realize productivity gains and remain viable in the competitive marketplace. One of the main initiatives that supports this strategy is the Advanced Computing Environment (ACE) initiative, which encompasses the planning, design, and implementation of a suite of services that updates the distributed computing environment. This initiative includes replacing out-of-warranty hardware and software products; upgrading existing technology and processes; and enhancing the stability, reliability, and availability of the existing infrastructure.

By rejuvenating aging and obsolete components of the distributed computing infrastructure, ACE reduces operational costs, increases levels of service, provides the Postal Service with a competitive advantage, and provides a framework for rapid deployment of business systems solutions. ACE renews all aspects of the distributed computing environment: user support, help desk support, application services, architecture, and governance. It upgrades 200,000 personal computers and 18,000 servers in a consistent manner—with a standardized approach to enterprise architecture and managed services.

In addition to ACE, the Associate Office Infrastructure, the Headquarters Infrastructure, the Field Infrastructure, Plant Upgrade / Wiring, and the Mobile Data Collection Devices are initiatives that support this strategy.

Milestones

- Replacement of workstations at Headquarters (2002 through 2003)
- Replacement of Headquarters-associated workstations at facilities (2003 through 2004)
- Replacement of workstations at field sites (2003 through 2005)
- Upgrade of the messaging system across the Postal Service (2002 through 2004)
- Consolidation of help desks (2002 through 2003)
- Reduction of contractor resources that provide technology support to the field (2003 through 2005)
- Upgrade of the Associate Office Infrastructure (2003 through 2005)
- Migration of legacy applications to Web-enabled systems (2002 through 2006)
- Replace Mobile Data Collection Device (2005 through 2007)
- Refresh of all components based on technology changes (2005 through 2009)

Metrics

- Reduce total cost of ownership on desktop computers by 25-40 percent
- Reduce application development times by 50 percent
- Significantly reduce security vulnerabilities
- Reduce deployment times for new applications by as much as 90 percent

Interdependencies

The ongoing effort to consolidate data, which is outlined in the Data Access and Integration section of this plan.

Obstacles

The size and complexity of the technology infrastructure offer significant challenges in that few organizations have a similar size and scope (implementations within the Postal Service are often the largest within the industry).

Substrategy 2: Upgraded mainframe computing infrastructure

Background

The mainframe computing environment is where the majority of the Postal Service's business computer processing takes place. Today this computing environment is located in Minneapolis, Minnesota, and San Mateo, California, with backup and disaster recovery sites in Raleigh, North Carolina. These computers house and process all of the databases for the corporation, including those that support over 1,200 applications that enable Postal Service customers, business partners, and postal managers to perform their day-to-day jobs. Items that require continual upgrades or replacement as industry changes are introduced are as follows: hardware, operating system software, application software, disk storage, and data warehouse.

The three major programs that support this strategy are Corporate-wide Software, eBusiness IT Infrastructure, and Enterprise Infrastructure Utilities.

Milestones

- Upgrade disk storage for additional backup capabilities (2003 through 2008)
- Upgrade and replace operating system software (Annually)
- Implement additional data warehouse capabilities (2003 through 2007)
- Replace or upgrade vendor application software releases (Annually)
- Replace mainframe computer hardware (2004 and 2007)

Metrics

- Reduce one-time support costs by 20 percent
- Improve speed of service
- Render data and information available on-demand

Interdependencies

The following initiatives which are outlined in the *Transformation Plan*: enhanced security across all technology, value-added services, universal computing connectivity, and data access and integration.

Obstacles

The size and complexity of the technology infrastructure offer significant challenges in that few organizations have a similar size and scope (implementations within the Postal Service are often the largest within the industry).

Substrategy 3: Upgraded midrange computing infrastructure

Background

Of the three levels of the technology computing environment, the midrange computing level is the least costly applications, operations, and support services. This is the newest computing environment in the industry and not all applications can run on this technology. Most companies use this environment to support the newest technological and application changes while not jeopardizing the legacy computing on the mainframe. Over time, approximately 30 percent of the workload from the mainframe environment will migrate to this midrange computer environment, because costs can be reduced.

The two major programs that support this strategy are the Postal Field Computing Infrastructure and the Mid-Range Systems Support.

Milestones

- Provide additional UNIX computing capabilities (2002 through 2005)
- Consolidate and replace all VAX computing (2002 through 2003)
- Establish improved UNIX production support expertise (2003 through 2006)

Metrics

- Total cost of application support is reduced
- All like computing is centralized
- Better application support is provided

Interdependencies

The Shared Services strategy and the Workforce Planning initiative.

Obstacles

The size and complexity of the technology infrastructure offer significant challenges in that few organizations have a similar size and scope (implementations within the Postal Service are often the largest within the industry).

Substrategy 4: Technical shared services

Background

This initiative leverages the infrastructure upgrades by improving information technology service offerings, including products, services, and processes. It is part of a larger Shared Services business model that the Postal Service is using for all support functions. Shared Services has been proven in a number of Fortune 500 organizations to increase organizational effectiveness, improve quality of services, reduce administrative workhours, and improve customer service levels, while realizing significant cost savings. Shared Services will utilize the upgraded infrastructure to allow the internal service areas in the Postal Service to be transformed from a purely administrative provider to a strategic partner within the organization.

In a continued effort to reduce the time it takes the technology organization to deliver systems and services to the organization, the Postal Service provides mechanisms for building integrated, rather than stove-piped applications. They are more efficient because they concentrate resources and expertise. Technical Shared Services are also readily adaptable to process improvements and performance measurement. Common examples of these services are data communications, transaction processing, and access control, applications development, consulting, customer support, deployment, and training.

Milestones

- Application development, enhancement maintenance service (2004 through 2008)
- Corporate software licensing and hardware (2002 through 2007)
- Customer support services — Help Desk (2004 through 2006)
- Data acquisition and presentation service (2003 through 2006)
- Data warehouse services (2003 through 2006)
- Secure file transfer services (2004)
- Data base support services (2002 through 2008)
- Disaster recovery service (2002 through 2007)
- Distributed enterprise management services (2005)
- Distributed hardware and software deployment and support (2002 through 2007)
- Host Computing Services (2002 through 2009)

Metrics

- Reduction in development costs
- Reduction in time to build systems
- Improved reporting
- Reduction in time required to respond to changes or challenges confronting the Postal Service

Interdependencies

Infrastructure upgrades and the integration of Shared Services initiatives across the enterprise.

Substrategy 5: Corporate shared services

Background

Corporate shared services focus on those initiatives that utilize the upgraded infrastructure to reinvent the Postal Service's back-office by reengineering human resources, finance, accounting, purchasing, and technology functions across the enterprise. Examples of corporate shared service initiatives include: the Standard Accounting Field Retail system, the Accounting Shared Services system, the Injury Compensation system, and Self Service activities, which are intranet-accessible.

Milestones

- Standard Accounting Field Retail (2002 through 2004)
- Accounting Shared Services (2002 through 2005)
- Injury Compensation (2003 through 2006)
- Self Service activities via the Postal Service Intranet (2003 through 2008)

Metrics

- Reduction in labor costs
- Reduction in time required to complete administrative activities
- Improved reporting
- Reduction in time required to respond to administrative changes or challenges

Interdependencies

Leveraging of the technology, infrastructure, and processes involved in all the various shared service initiatives from each business area.

Provide Universal Computing Connectivity

Overarching Objective

The Postal Service must continue to leverage its greatest asset by expanding the uses and the availability of the network to provide a means of reducing the Postal Service operational, training, travel, and other expenses. Expanding the use of the network will also ensure that postal employees are as productive as possible and can be “connected”—anywhere, anytime—providing significant cost savings.

Real labor cost savings will be realized as the network continues its support function for the finance and human resources areas, and becomes an integral work conduit in the operations area. An up-to-date, robust network will improve productivity and replace workhours in virtually every area of the Postal Service. To support all Postal Service, business partners, and interagency partners, the Postal Service requires a highly reliable and secure network—for voice, data, and video transmissions—available twenty four hours a day, seven days a week.

Strategy: Expand core / backbone, wide area network, and local area networks to provide universal computing connectivity

Substrategy 1: Consolidated voice, data, and video network

Background

The network continues to play an increasingly important role in all business areas of the Postal Service, from finance to human resources to mail processing to business partners. Internal, external, and interagency partners also rely on this network. With these demands on the network, upgrades are imperative if the network is to continue to meet these service requirements.

The current network infrastructure supports over 35,000 locations via 15,000 dedicated landlines and VSAT connections and over 38,000 dial-up, cable, and high-speed remote connections. While it is highly reliable and meets many of today’s postal requirements, it falls short in other areas. There are many video, voice, and other high-speed requirements that the current network infrastructure cannot meet. Not being able to meet these requirements severely limits the operational uses of the network.

The three programs that support this strategy are Telecommunications Network Operations, Telecommunications Voice Service, and Telecommunications Equipment and Wiring.

Milestones

- Evaluate all point to point existing and proposed networks (2003 through 2004)
- Consolidate mail processing networks (FRES, RBCS, PARS, and APPS) into the current MNS network (2003 through 2008)
- Develop Request for Proposal/Statement of Work for high-speed managed network services (2003 through 2006)

- Evaluate new managed network services proposals (2004 through 2006)
- Award new managed network services contract (2005 through 2006)
- Expand network services to other government agencies (2005 through 2008)

Metrics

- Track number of users, devices, and types of devices (data, voice, video, servers, desktop, laptop, and wireless devices) supported
- Provide availability and response time statistics

Interdependencies

The investigation of the use of a shared, high-speed network to support the current and proposed mail operations point-to-point networks.

Obstacles

The size and complexity of the technology infrastructure offer significant challenges in that few organizations have a similar size and scope (implementations within the Postal Service are often the largest within the industry).

Substrategy 2: Wireless technology

Background

In providing connectivity anywhere / anytime to its two thousand line managers and executives, the Postal Service has a wireless initiative underway that supports e-mail, calendar features, pager capabilities, work tasks management, address book information, and Internet access all in one device. The next generation of this technology will combine cell phone services. This wireless service will also enable Information Technology to be able to offer business continuity of operations for contingency purposes. Today, approximately two hundred users are connected via wireless technology. In addition to receiving e-mail anytime / anywhere, these wireless devices provide alerts (both visually and audibly) on the status of major applications within the postal environment. Such connectivity is exceptionally critical to the Postal Service since managers supervise the mail twenty four hours a day, seven days a week. The Postal Service is also planning to use this wireless system for disaster recovery operations. Since these devices work outside of the e-mail system, communication to key personnel can be maintained in the event of an emergency. The next logical step is access to mission critical applications via wireless technology using the same devices. This wireless access will provide a seamless view of an application regardless of whether the manager is at his or her desk or walking the floor of a plant. The future for these devices within the Postal Service is bright. As the costs of airtime and devices fall, it is becoming increasingly cost-effective to use wireless devices to conduct day-to-day business. The speed of information flow for wireless devices is also expected to increase dramatically over the next few years, allowing for more sophisticated applications.

Milestones

- Create wireless solution for daily management and contingency plans (2002 through 2003)
- Deploy wireless solution to all headquarters officers and managers (2002 through 2004)
- Deploy wireless solution to all field officers and managers (2003 through 2004)
- Provide and implement cost savings capabilities (2003 through 2007)

Metrics

- Usage of the wireless devices
- Increased productivity for management
- Savings of management time
- Efficiencies in problem resolution for operational issues

Interdependencies

Infrastructure upgrades

Obstacles

The size and complexity of the technology infrastructure offer significant challenges in that few organizations have a similar size and scope (implementations within the Postal Service are often the largest within the industry).

Postal Inspection Service — Safety

Overarching Objective

People are the greatest asset of the Postal Inspection Service. The safety of postal employees, customers and facilities is paramount for the Postal Inspection Service¹ in ensuring a safe work and business environment.

Background

Through the years, the Postal Inspection Service has established itself as uniquely qualified to provide safety and security for Postal Service employees and customers. This has been accomplished through its law enforcement and at one time, audit authority. The dedication of Inspection Service employees, their commitment to the mission, and the quality of their work has provided the Postal Service and the U.S. government with unquestioned value.

In the past, the Postal Service's greatest threats against safety came in the form of criminal acts such as robberies and assaults of employees and customers. Recent events have added terrorism to the list. The Inspection Service must continue to enhance its services, both in number and rigor, in order to protect postal employees

¹ The Postal Inspection Service is a highly specialized, professional organization performing investigative and security functions essential to a stable and sound postal system. As fact-finding and investigative agents, Postal Inspectors are federal law enforcement officers who carry firearms, make arrests, and serve federal search warrants and subpoenas. Inspectors work closely with U.S. attorneys, other law enforcement agencies and local prosecutors to investigate postal cases and prepare them for court. There are approximately 2,000 Postal Inspectors stationed throughout the United States who enforce more than 200 federal laws covering investigations of crimes that adversely affect or fraudulently use the U.S. Mail and postal system.

and customers. Through its unique role of providing security prevention and investigative services, the Inspection Service strives to foster a safe working environment and make every effort to prevent injury or death.

Strategy: Ensure a safe, secure, and drug-free work environment

Substrategy 1: Reduce and deter employee-on-employee assaults and credible threats

- Partner with the Postal Service to establish Threat Assessment Teams (TATs) in each performance cluster, participate in orientations for newly formed TATs, train with the TAT and attend regularly scheduled TAT meetings
- Coordinate with TATs in preventive and investigative efforts to prevent employee-on-employee credible threats and assaults
- Provide immediate response and investigation for all assaults
- Seek prosecution and removal of all employees responsible for all assaults

Benefits

This program will provide a safer working environment for postal employees; increase employee morale, well being and productivity through reduced fear and stress; provide a safer business environment for customers; and enhance the Postal Service image in the eyes of the public.

Substrategy 2: Deter robberies of postal employees and facilities

- Collaborate with Security Control Officers to perform risk assessments of facilities and install countermeasures
- Develop and implement preventive, deterrent, and investigative strategies for robberies
- Conduct priority investigations when robberies occur to solve all robberies

Benefits

This program includes a safer working environment for employees and business customers, a reduction in serious injuries and deaths, and increased moral of employees through reduced fear and stress.

Substrategy 3: Reduce and deter illegal drugs in the postal environment

- Identify facilities with workplace drug problems and implement preventive, deterrent and investigative strategies
- Maintain an intelligence system to document information regarding narcotics problems in order to track problems within a specific facility

In addition to the above substrategies, the Inspection Service will emphasize programs, which address the immediate needs of the Postal Service due to terrorist and bio-terrorist attacks against the Postal Service and the American public. The programs, while continually active, are being reassessed to ensure proper service levels.

- Provide security at postal facilities where risk, vulnerability, and history demonstrate the need for an armed presence
- Ensure the security of the mail during sanitization procedures
- Develop proactive mail screening techniques to detect hazardous mailings
- Conduct and assist other agencies in the investigation of terrorist threats
- Continue to support the hazardous materials program (HazMat), by providing enforcement support for violations under the criminal code (Title 18 U.S.C.)
- Continue to provide the technical expertise in the Postal Service Aviation Security Program
- Establish and enforce a national photo identification program for Postal Service personnel
- Coordinate with personnel offices to ensure the Postal Service hiring practices include proper background investigations

Benefits

The benefits of this substrategy include a safe and healthy work environment for postal employees; an increase in morale and productivity; a reduction in crime in the postal environment, including crimes of violence; reduced accidents; and a reduction in unscheduled absences and workers' compensation claims. Also, this program includes improved safety for postal employees through enhanced perimeter security and reduced assaults, robberies, and other criminal activity.

In addition, safer postal facilities and operations, enhanced expertise and readiness in responding to critical incidents, and less risk and exposure for postal employees and customers to hazardous situations and materials will also be realized.

Metrics

The following three charts depict the trends and results of Inspection Service investigative work in recent years. Success in these programs has helped sustain the trust the public puts in the U.S. mail system.

CHART 1: ASSAULTS AND THREATS

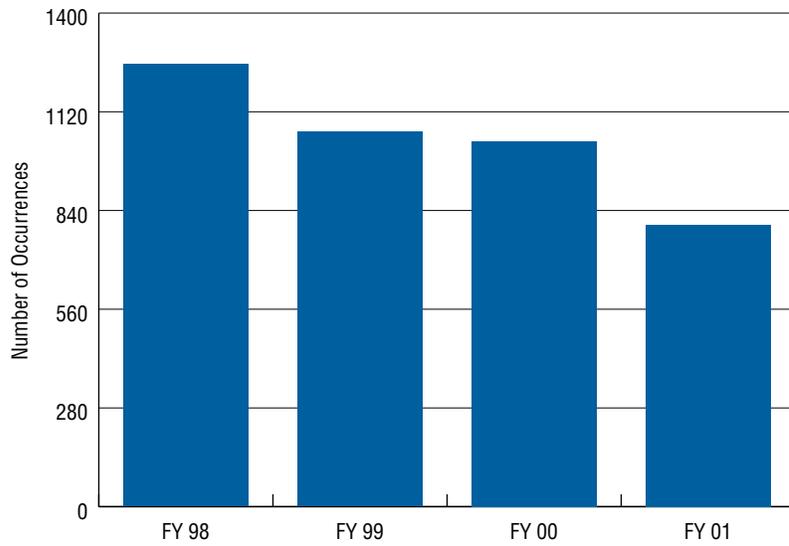


CHART 2: ROBBERIES

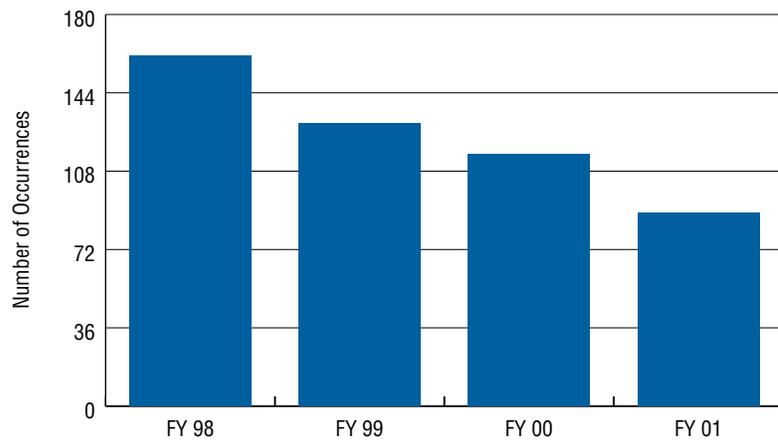
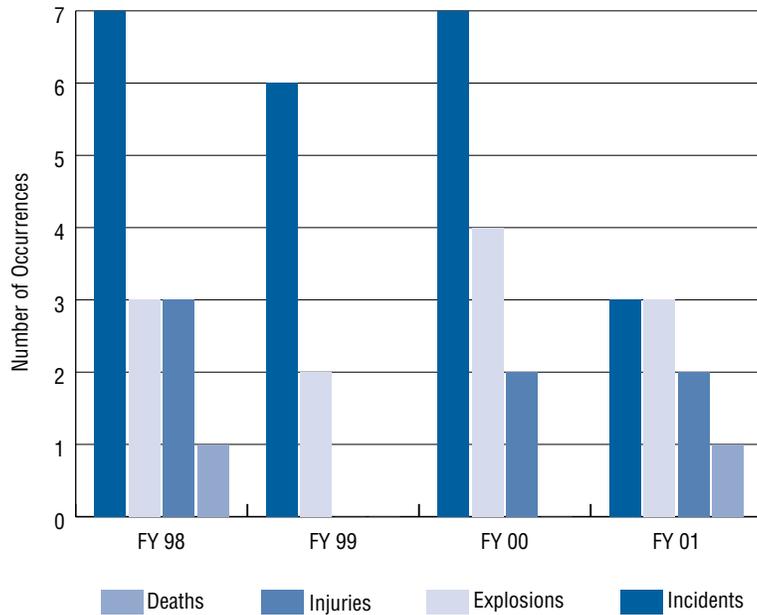


CHART 3: MAIL BOMB INCIDENTS



Interdependencies

While the Inspection Service conducts investigations and makes recommendations concerning security initiatives the implementation is the responsibility of Postal Service management. The Inspection Service also depends on the cooperation of postal managers and bargaining-unit officials and employees to participate in security initiatives.

The Inspection Service works with multiple federal, state, and local law enforcement agencies to complete successful investigations in these program areas. Support is also obtained from intra-agency groups such as the Forensic and Technology Support division, Career Development division, and Information Technology division.

Obstacles

Hazardous Mailings

- New threats posed by bioterrorism
- Early detection of biohazards in the mail stream
- Lack of industry knowledge regarding biohazards

Postal Inspection Service — Security

Overarching Objective

Providing for the security of the mail and postal products, services and assets is integral to the Inspection Service’s mission to protect the Postal Service from criminal attack.

Background

Inspection Service security programs address crimes affecting the mail, postal

operations, and revenue which can undermine postal operations and erode the financial stability of the Postal Service. The American people have relied on the U. S. mail to conduct the commerce of the nation and the value added by the Inspection Service must ensure this tradition continues.

Combating mail theft is essential to ensuring that the Postal Service is successful in its core function of delivery. Mail theft techniques have become more sophisticated and widely divergent in some geographic areas. Criminals no longer focus on taking the single piece of mail from the mailbox, but focus on large volumes of mail, from which they obtain information useful to perpetrate other criminal endeavors. While the Inspection Service was successful in past years in reducing the number of these volume thefts, they have resurfaced in certain geographical areas. Investigative attentions have been focused to address the areas with the most severe problems. At the same time, control of the problems in other areas must also be maintained to avoid a reoccurrence of a national problem.

Given the difficult financial position of the Postal Service, the Inspection Service must remain vigilant in investigating and preventing any crime, from both internal and external perspectives, which may negatively impact postal revenues. These crimes include embezzlements, burglaries, workers' compensation fraud and schemes to underpay postage. Now more than ever, the Inspection Service must work to ensure the security of the mail while in transit. This is not only a security issue, but overlaps into ensuring the safety of postal employees and customers.

Strategy 1: Reduce theft of mail

Substrategy 1: Reduce and deter attacks on postal vehicles, apartment panels, collection boxes, neighborhood delivery collection box units and collection box units

- Target investigative and preventive attention
- Implement effective countermeasures and strategies
- All divisions will monitor mail theft trends and aggressively address negative trends

Substrategy 2: Identify and resolve domestic and international in-transit mail theft

- Identify domestic and international airports with in-transit mail theft problems
- Implement preventive, deterrent, and investigative strategies
- Ensure only Postal Service related ground-handling employees have access to mail
- Conduct airport mail security reviews

Substrategy 3: Reduce and deter mail theft-related identity theft and identity takeover crimes

- Implement preventive, deterrent and investigative strategies
- Identify post office boxes or individual commercial mail receiving agency boxes used to commit identity theft
- Where appropriate, pursue administrative actions

Benefits

This program will reduce mail theft, identity takeover schemes and customer losses, thereby increasing customer trust and confidence in the Postal Service. Our efforts at airports will also enhance the security of international mail.

Strategy 2: Reduce and deter criminal attack of postal products, services and assets

Substrategy 1: Reduce and deter embezzlements

- Increase investigative attention to embezzlement of postal funds at retail stores and other offices under Segmented Inventory Accountability

Substrategy 2: Reduce and deter criminal misuse of the Postal Service's workers' compensation program and reduce long-term compensation cost

- Identify criminal misuse of the Postal Service's workers' compensation program

Substrategy 3: Reduce and deter postage fraud schemes

- Identify high-risk postage fraud areas and prosecute perpetrators through criminal and civil actions

The benefits of these strategies will protect postal revenue by reducing the number of employee embezzlements, increase the ability to investigate embezzlements related to new financial systems, reduce fraudulent claims by employees, assist in the maintenance of the financial health of the Postal Service and reduce the Postal Service's vulnerability to postage fraud schemes.

In addition to the above strategies the Inspection Service will emphasize programs, which address the immediate needs of the Postal Service due to terrorist and bioterrorist attacks against the Postal Service and the American public. The programs, while continually active, are being reassessed to ensure proper service levels.

Substrategy 4: Ensure sanctity and security of U.S. mail

- Evaluate compliance with security programs to ensure the sanctity of U.S. mail handled by the Postal Service and contractors
- Ensure the accuracy and reliability of the Postal Service mail condition reports used by the Postal Service and contractors
- Identify security related issues, concerns, or conditions that require corrective action by postal management
- Security escorts of high-value shipments such as registered mail and postal remittances when necessary

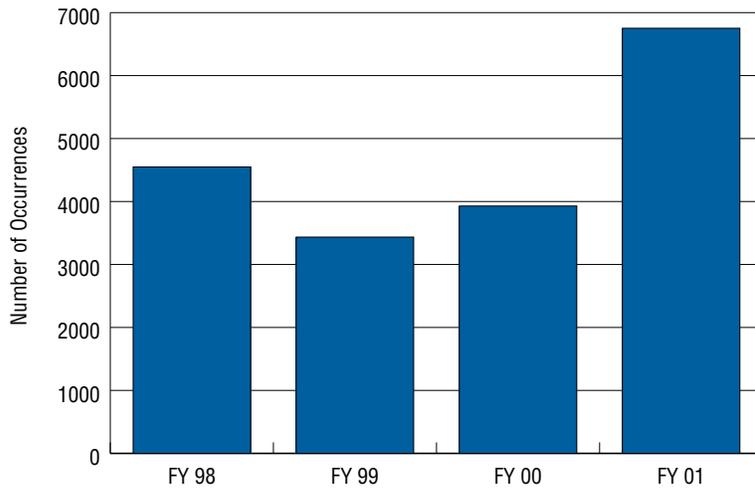
Substrategy 5: Assist postal management in the deployment and implementation of new safety and security procedures and technology

Investigative efforts in these areas will assist in promoting a secure business environment for postal customers and maximize the security of postal facilities, products and services. Additionally, the Inspection Service will work in an advisory capacity with postal management concerning new technology requirements to address the safety and security of employees and the mail.

Metrics

Charts four through seven depict the trends and results of Inspection Service investigative work in recent years. The Inspection Service has done an outstanding job in the area of burglaries, but must continue to monitor occurrences to ensure the program is maintained. In other investigative programs, the Inspection Service needs to maintain aggressive investigative and preventive attention.

CHART 4: VOLUME THEFTS



National mail thefts from receptacles or deposit points serving multiple customers.

CHART 5: BURGLARIES

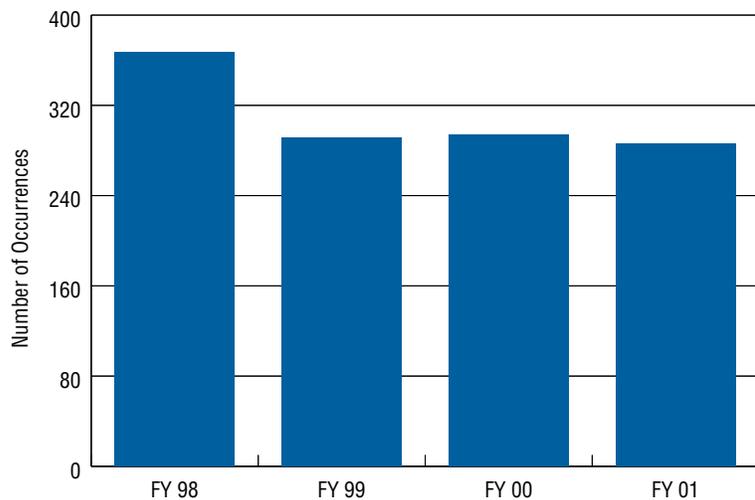


CHART 6: EMBEZZLEMENTS

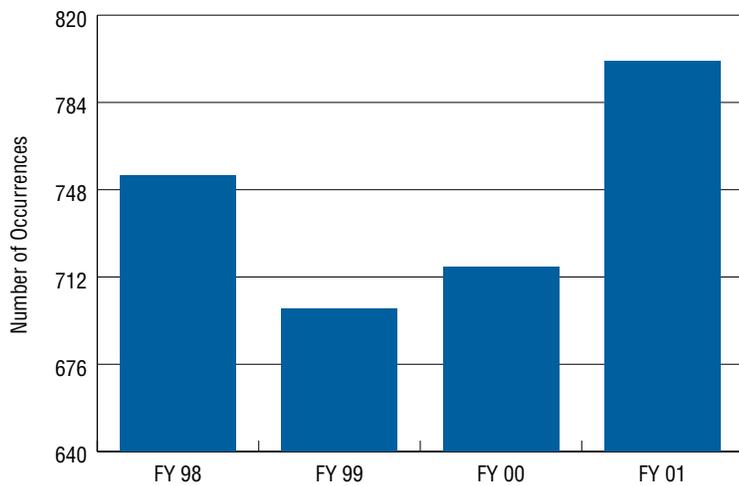
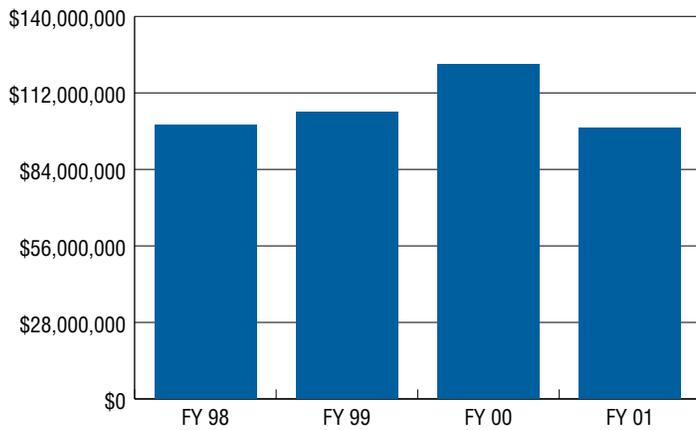


CHART 7: WORKERS' COMPENSATION FRAUD



Compensation and COP savings identified through investigations.

Interdependencies

While the Inspection Service conducts investigations and makes recommendations concerning security initiatives the implementation is the responsibility of Postal Service management. The Inspection Service also depends on the cooperation of Postal managers to implement recommendations and to apply administrative actions when necessary.

The Inspection Service works with multiple federal, state, and local law enforcement agencies to complete successful criminal investigations in these program areas. Support is also obtained from intra-agency groups such as Forensic and Technology Support division, Career Development division, and Information Technology division.

Obstacles

Mail Theft

- Implementation of all preventative initiatives
- Loss of expertise through attrition
- Under-utilization of technical tools
- Timeliness and quality of mail loss data from customers and business partners

Revenue and Asset Protection

- Investigative leads rely heavily on tips

Sanctity of the Mail

- Cooperation with business partners
- Enforcement of regulations and compliance by postal managers

Postal Inspection Service — Integrity

Overarching Objective

The Inspection Service protects the integrity of the Postal Service by combating the furtherance of crimes using the postal system.

Background

The Postal Inspection Service has investigative responsibility to protect the postal system from criminal activities. This is accomplished through criminal investigations in the areas of mail fraud, illegal drugs in the mail, money laundering and child exploitation.

The Inspection Service often takes the lead in responding to mail fraud schemes relating to telemarketing, mail orders, insurance and investments. Mail fraud is expected to increase as more promoters take advantage of the perceived anonymity of the Internet. These cases ultimately involve the use of the mail. The Inspection Service must maintain its proficiency with traditional mail fraud investigations, while improving skills related to Internet cases.

The Postal Service cannot allow its vast distribution and delivery network to be used to assist criminals in illegal activities such as the transportation of illegal substances and child pornography or to use its financial network to launder funds obtained through illegal activities. Inspection Service investigative attention in these areas fulfills the mandate to sustain America's trust in the U.S. mail.

Strategy 1: Reduce the use of the mail to defraud consumers, businesses and government agencies

Substrategy: Reduce and deter the use of the U.S. mail for the procurement or delivery of materials that promote the sexual exploitation of children

- Continue to support a nationwide child sexual exploitation initiative with the Department of Justice
- Enhance use of the Internet as an investigative tool
- Implement prevention and education strategies to protect children from sexual exploitation

Benefits

This program will ensure fewer children are at risk for sexual exploitation, identify and stop child molesters, assist in rescuing children from ongoing sexual abuse, and reduce child pornography in the mail and the Internet.

Strategy 2: Reduce and deter the use of the postal system for prohibited, illegal, and dangerous mailings

Substrategy 1: Reduce and deter multistate domestic and international telemarketing operations and direct mail operations

Identify and disrupt multistate domestic and international fraudulent telemarketing mailing operations and direct mail solicitations with call-back numbers.

Substrategy 2: Reduce and deter deceptive mailing operations

Identify and disrupt deceptive mailing operations by utilizing information from established contacts, referrals, the Fraud Complaint System (FCS), Consumer Sentinel, Publication Monitoring or those investigations referred by the national Postal headquarters Deceptive Mail Enforcement Team.

Benefits

This program will improve customer confidence in the integrity of the postal system through reduced incidents of fraudulent use of the mail and by reducing the economic losses to individuals, customers, businesses and government agencies stemming from fraudulent activities using the mail.

Substrategy 3: Reduce and deter the use of the nation's mail system by organized groups to transport illegal narcotics

- Conduct national drug interdictions coordinated by Postal Service Headquarters
- Identify and disrupt organized, illegal drug shipment groups using the mails
- Focus attention on interagency task force interdictions of mail and private carriers

Benefits

This program will include increased safety of postal employees from violence related to drugs transported through the mail and a decrease in the use of the mail to ship illegal drugs.

Substrategy 4: Reduce and deter the use of U.S. Postal Money Orders to launder money by disrupting money laundering operations

Identify and disrupt money laundering operations in high intensity financial crime areas and other geographical areas identified through intelligence and analysis of statistical data.

Benefits

This program will include reduced use of the postal system for money laundering operations, protection of the Postal Service's Money Order system from illegal activity, and disrupting the ability of criminal groups from profiting from illicit proceeds, thereby instilling trust in the Postal Service.

Metrics

The table below depicts the trends and results of Inspection Service investigative work in recent years. Success in these programs has helped sustain the trust the public puts in the U.S. Mail system.

| | | | |
|----------------------------------|----------------|----------------|----------------|
| Mail Fraud | | | |
| | | FY 2000 | FY 2001 |
| Arrests | | 1,633 | 1,691 |
| Convictions | | 1,377 | 1,477 |
| Illegal Drugs in the Mail | | | |
| | FY 1999 | FY 2000 | FY 2001 |
| Arrests | | 1,537 | 1,575 |
| Drugs (lbs.) | | 15,436 | 9,335 |
| Money (\$ Million) | | 6.5 | 3.5 |
| Money Laundering | | | |
| | | FY 2000 | FY 2001 |
| Arrests | | .96 | .111 |
| Convictions | | .42 | .52 |
| Child Exploitation | | | |
| | FY 1999 | FY 2000 | FY 2001 |
| Arrests | | .163 | .257 |

Interdependencies

The Inspection Service works with multiple federal, state, and local law enforcement agencies to complete successful investigations in these program areas. Support is also obtained from intra-agency groups such as Forensic and Technology Support division, Career Development division, and Information Technology division.

Obstacles

Child Pornography

Task force dependencies

Mail Fraud

- Trusting nature of the general public
- Reluctance of businesses to share proprietary information
- Mobility of criminals
- Increased use of the Internet

Illegal Drugs in the Mail

- Jurisdictional overlap

Money Laundering

- Effective inter-agency cooperation

Future Plans

With the advent of moderate postal reform, the Inspection Service's role of providing security and conducting criminal investigations should remain relatively stable. The need for these services transcends all legislative frameworks. Should the Postal Service lose the postal monopoly on some products, it might become necessary to revisit the Inspection Service's statutory authority, especially for deregulated product lines.

The Inspection Service must also consider the financial situation of the Postal Service, particularly the impact of declining revenue. Loss of revenue impacts funding for all postal operations including the Inspection Service. In light of new challenges due to terrorism and possible jurisdictional changes brought on by structural changes in other law enforcement agencies, such as the FBI's focus on counterterrorism, adequate funding must be available to meet the investigative demands.

Some possible strategies to meet this situation include:

- Evaluate the impact of proposed legislative changes on the Inspection Service's operations
- Strengthen liaisons with the Postal Service management to ensure the Inspection Service is meeting their needs
- Strengthen relations with Congress to ensure legislative adjustments allow the Inspection Service to operate in a manner conducive to the needs of the Postal Service
- Maintain liaison with the Department of Justice to be responsive to jurisdictional needs

- Prepare draft legislation to enable the Inspection Service to fulfill its mission
- Continued development of an intelligence analyst support function
- Enhance human resource capacity to ensure the appropriate placement and skill level of personnel
- Consider alternate sources of funding and appropriations

Inspection Service personnel are trained to address law enforcement and security issues and also possess an extensive knowledge of postal operations. This combined knowledge has added value to the Postal Service in providing service to its customers.

If the Postal Service were totally deregulated, the role of the Inspection Service would be in question. The need for an internal security program would still exist, much like any private industry needs corporate security. However, jurisdictional questions would arise and investigative programs would have to be reevaluated. Activities mandated by statute would have to be reviewed.

Some possible strategies in addition to those under moderate reform include:

- Consider expansion of jurisdiction to encompass private sector
- Adjust focus to corporate security
- Focus on meeting the needs of customers and consumers by being service driven and developing marketing strategies

Privacy

Overarching Objective

Ensure that the Postal Service maintains its trusted brand and provides top-rate privacy protection.

Background

The Privacy Office, established in November 2000, is responsible for ensuring that the Postal Service maintains its trusted brand, developed over its 225-year history, regarding safeguarding privacy. The privacy landscape is evolving. To ensure the Postal Service provides top-rate privacy protections in today's world, the Privacy Office keeps up with developing legal and policy frameworks, new technologies, and business models and practices. The Privacy Office is also responsible for managing Privacy Act and Freedom of Information Act (FOIA) compliance.

To tackle these issues, the Postal Service employs a three-part program—people, policies, and processes. The Postal Service was among the first federal agencies to appoint a Chief Privacy Officer (CPO), who ensures that appropriate cross-functional groups are involved with setting policies and processes. The Privacy Office seeks to establish and implement privacy policies that reflect best practices of both government and industry. The office also continues to develop processes to ensure compliance with statutes and policies.

The Postal Service complies with both federal requirements and commercial guidelines. Adherence to federal privacy laws strengthens the Postal Service trusted brand, and allows the Postal Service to offer privacy assurances, backed by federal law, which private sector competitors do not. However, federal laws limit the ability of the Postal Service to collect, use, and sell customer data like other businesses. Federal privacy and FOIA laws also impose certain compliance requirements on the Postal Service that do not apply to private sector competitors.

Strategy 1: Standardize privacy policies and processes

- Establish enterprise-wide privacy policies across channels and customer segments
- Create uniform privacy clauses for contracts and alliances
- Establish a uniform privacy and FOIA handbook and training

Strategy 2: Streamline compliance procedures to reduce costs and increase productivity by saving time

- Rewrite all customer Privacy Act Systems of Records
- Simplify Privacy Act clearances and improve FOIA tracking

Strategy 3: Work with internal and external groups to ensure that privacy is built into data-oriented initiatives

- Establish and communicate standard processes for business drivers
- Work with drivers of personalization initiatives (marketing efforts based on customer data) and intelligent mail service (knowledge of mailer and its mail throughout the postal system).

Metrics

- Reduction in labor costs through streamlined procedures
- Increased compliance through standard processes
- Increased value in Postal product and service offerings to customers through proper use of customer data
- Recognition of the Postal Service as developer of best-in-class privacy policies and practices

Interdependencies

While the Privacy Office is responsible for developing privacy policies and processes, the office coordinates heavily with other functions in this development and to ensure successful implementation and compliance. The standardization and streamlining activities are significant undertakings, and require extensive coordination with other departments. Standard policies must be developed carefully to promote the Postal Service trusted brand, but yet be workable for business units. Personalization and intelligent mail activities will require buy-in from stakeholders, customers, and mail recipients.

Moderate reform. The Postal Service would need to ensure the appropriate transition and sharing of information between competitive and noncompetitive business lines, within any parameters set by Congress. Competitive business units would need to embrace commercial practices, while still complying with applicable statutes and voluntary policies that the Postal Service adopts.

Structural reform. In a more commercial setting, the Postal Service would have more freedom to set policies regarding use of customer data—these issues should be examined very carefully, taking into account brand strategy and customer expectations. The Postal Service would need to balance greater flexibility, business needs, and acceptance by customers. Internally, the Privacy Office would continue to need substantial integration with key stakeholders. The focus of the privacy program would be on establishing appropriate policies and processes in this environment. Regulatory requirements that do not support the brand could be eliminated.

Obstacles

The use and transfer of data may be hampered, and, under structural reform, the Postal Service brand may be impacted. There is considerable sensitivity surrounding Postal Service customer data as well as expectations around use of that data.

Moderate reform. Under moderate reform, there may be continuing restrictions on how customer data is used, and new restrictions placed on the transfer of data between business units. Competitors and regulators may object if new business units are able to transport customer data from existing units, compromising the Postal Service's ability to implement strategies. Moderate reform, which may create these two separate business units, could hamper successful cross-business efforts by building a firewall between them.

Structural reform. The Postal Service brand image as a trusted third party provides strong privacy and security protections. Some of that brand value is linked to being a government entity that is required to adhere to federal privacy laws. Without government backing and enforcement, the Postal Service risks losing some of its credibility as a trusted third party. Policies the Postal Service adopts may also impact the brand.

