U.S. Postal Service Office of Inspector General

Congressional Budget Justification

FY 2017

U.S. Postal Service Office of Inspector General

Fiscal Year 2017 Budget Submission Outline

Preface

In keeping with the President's agenda for growth and opportunity and to reduce spending on lower priority programs, the Office of Inspector General's (OIG) budget request of $258,800,000 reflects a 4.1 percent increase from our Fiscal Year (FY) 2016 budget. This budget increase covers inflation for salaries and benefits, rent, and other non-personnel costs. It will further allow the OIG to appropriately adjust our level of support to safeguard postal systems and information from critical cybersecurity vulnerabilities; detect, prosecute, and recover funds from claimant and provider fraud for the Postal Service; and fund a $776,400 assessment to support the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

Cybersecurity has been identified as one of the most serious economic and national security challenges we face as a nation. The Postal Service fell victim to a cyber-intrusion in September 2014, compromising the personally identifiable information of more than 800,000 current and former employees, compensation records, and customer inquiries. Our work was very influential in the initial identification of the breach and our audit and investigative efforts remain critical in cybersecurity.

The Postal Service breach and cyber-attacks at other federal entities have led to a growing focus on cybersecurity throughout the government. The Postal Service has one of the largest computer networks in the world, which handles more than 13 million emails a day — more than 4 billion annually — delivered to nearly 211,000 email accounts. In addition, the Postal Service maintains 47,000 point of sale terminals nationwide, and more than 340 million credit and debit card transactions are processed annually in Post Offices and through usps.com. The direct cost of another attack on the Postal Service could potentially cost millions of additional dollars and have a further negative impact to the Postal Service brand.

To help protect against the ongoing threat of future intrusions into the Postal Service network, the OIG proposes to fill three positions in this area. The Office of Investigations' (OI) Computer Crimes Unit (CCU) would fill one vacant position and the Office of Audit's (OA) Information Technology Directorate (ITD) would fill two vacant positions. These positions would allow OI and OA to conduct investigations; vulnerability scanning and penetration testing; and increase analytics efforts to evaluate and secure data.

Along with cybersecurity threats, the Postal Service continues to be at risk to claimant and provider fraud. The Postal Service is the largest single contributor to the Department of Labor's (DOL) Office of Worker's Compensation Program (OWCP). In

2014, the Postal Service paid $1.32 billion in Federal Employees' Compensation Act (FECA) related benefits. In the same year, the Postal Service estimated its total liability for future workers' compensation costs to be $17.1 billion. These disability payments are funded through Postal Service customers rather than tax dollars, and any portion of those funds lost to fraud by claimants or providers has a direct impact on the Postal Service and its customers.

We propose expanding our program by filling six positions and establishing a larger network of experienced claimant and provider fraud special agents across the country. These positions would be distributed across major field offices and our Major Fraud Investigations Division (MFID).

In FY 2014, our claimant and provider fraud investigations resulted in more than $275 million in direct cost reductions and over $35 million in fines and restitutions paid to the Postal Service. This amounts to more than the entire FY 2014 OIG annual budget. We have achieved $262 million in direct cost reductions and $7.4 million in fines and restitutions payable to the Postal Service.

This growth in OIG results is both an indication of our growing focus on claimant and provider fraud and the growing potential for fraud that exists throughout the program. Since October 1, 2009, the OIG has achieved nearly $1.5 billion in direct financial impact related to disability fraud against the Postal Service and reduced or eliminated benefits for approximately 1,800 claimants.

Because of our success, the Postal Service has encouraged the OIG for the past several years to shift additional resources to address these large threats of provider and claimant fraud. They have agreed to more aggressively address simple misconduct issues through their management structure to allow the redeployment of the OIG resources to claimant and provider fraud cases. In addition, we received over 300 requests from the Department of Justice in FY 2014 to join task forces investigating these types of frauds, and resolving many of these could have a significant impact on the Postal Service. Because these task force cases require highly experienced and capable special agents, as well as a long-term investment in investigative resources, the OIG needs to increase the number of tools and agents available to participate in these cases.

Increasingly, OIGs are using data analytics to develop evidence of such crimes and the Digital Accountability and Transparency Act is expected to enable larger and more sophisticated efforts to identify these crimes across the government. Our agency has been a leader in this area. We have developed a number of data analytic models with visualization of the model output in our Risk Assessment Data Repository (RADR) which helps to more quickly identify fraud (See Figures 1 and 2). A number of agencies

are using our tools as models for their own efforts and the DOL recently contracted to duplicate our healthcare data analytic models in its own infrastructure.

Figure 1: Risk Assessment Data Repository (RADR)

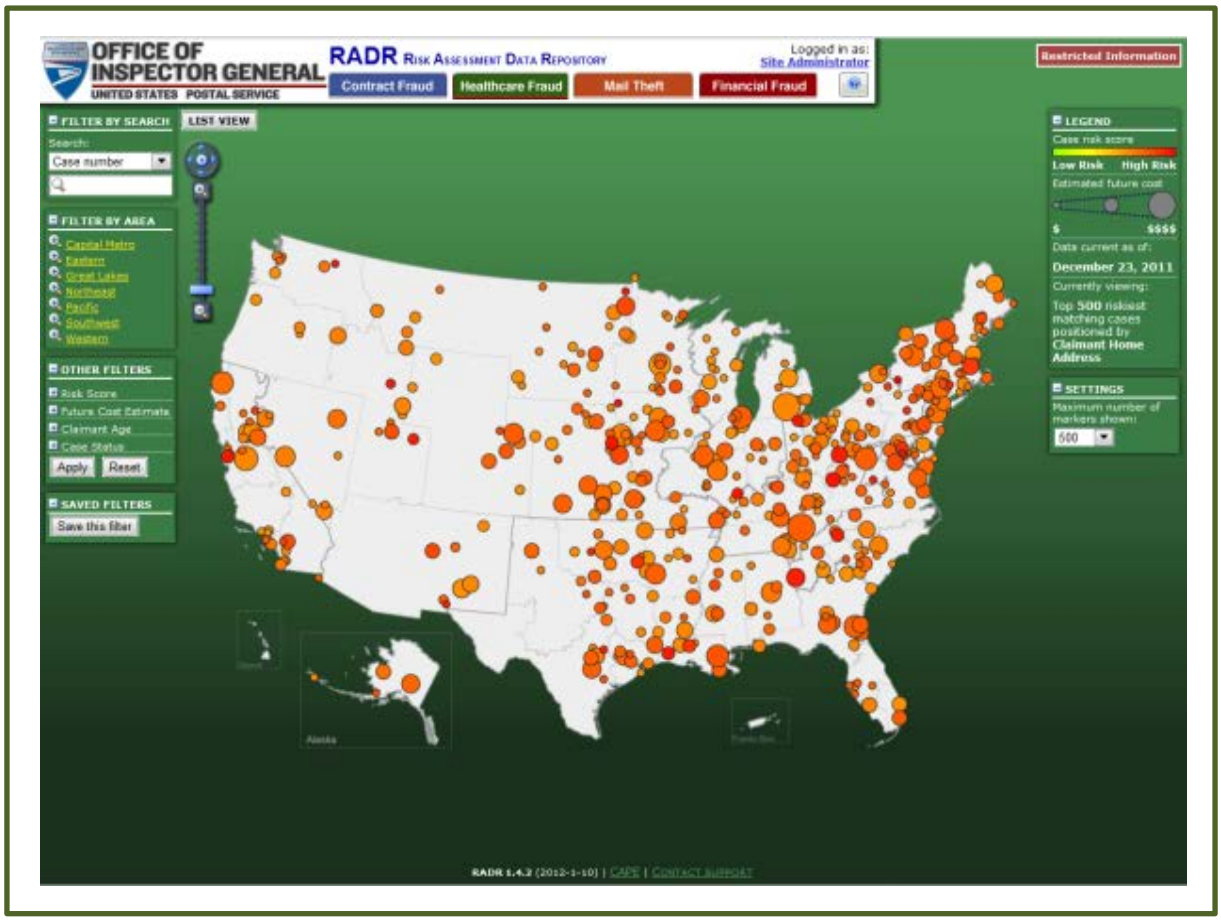


Figure 2: Risk Assessment Data Repository (RADR)

There is no doubt that cyber-attacks and massive provider and claimant fraud are occurring every day and our ability to detect, prosecute and recover is only limited by the resources we are able to invest in it. Our budget request for FY 2017 is the minimum amount we need to maintain our capacity to carry out our duties to help prevent fraud, waste, and abuse.

Table of Contents

Section 1 – Purpose

A. Mission Statement, Vision, and Values

The mission of the U.S. Postal Service Office of Inspector General (OIG) is to promote integrity and accountability by delivering optimal value to the Postal Service. The OIG ensures its stakeholders, the Congress, Board of Governors, and Postal Service management, are informed of areas of improvement, fraud, waste, and deficiencies, and are provided recommendations that enhance operational efficiencies.

In April 2013, the Postal Service published its 5-year business plan, which articulated five key restructuring objectives:

- Preserve the ability to provide and finance secure, reliable, and affordable universal delivery service
- Further economic growth and enhance commerce
- Implement comprehensive transformation for a sustainable financial future
- Protect U.S. taxpayers (avoid Federal funding and appropriations)
- Maintain fairness to employees and customers

To help the Postal Service with its initiatives and efforts to address its challenges, the OIG has invested in a diverse, highly productive work-force guided by a shared vision and sound values.

Our Vision:

- Performance to deliver value
- Passion for our mission
- Pride in our employees

Our Values

- Results
- Innovation
- Leadership and Professionalism
- Knowledge
- Flexibility

The OIG sets challenging goals that add value by identifying cost reduction opportunities and operations improvements, which support Postal Service efforts to become a leaner, smarter, and more agile organization with the goal of returning to financial stability and profitability. The OIG also seeks ways to improve operational integrity and to reduce the risk of revenue loss by detecting and preventing potential

fraud, waste, and abuse activities. Detection and prevention are accomplished by conducting independent, timely, high-quality audits, and by investigating allegations of fraud, theft, violations of criminal and civil statutes, and administrative misconduct.

The OIG has aligned mission resources to promote economy, efficiency, and effectiveness and concentrates on areas that are high risk for the Postal Service. Our Office of Audit will continue to focus on impactful operational recommendations, identifying cost savings, and increasing Postal revenue opportunities. Our Office of Investigations will continue to help prevent fraud and protect Postal assets by identifying and investigating high quality cases to minimize loss and maximize recoveries for the Postal Service.

B. Budget Summary

In accordance with the requirements of Public Law 110-409, the Inspector General Reform Act of 2008 (as amended), the U.S. Postal Service Office of Inspector General submits the following information related to its requested budget for FY 2017:

- The aggregate budget request for the operations of OIG is $258,800,000
- The portion of the budget needed for OIG training is $2,667,213.
- The portion of the above training budget needed to support CIGIE is $776,400, which is 0.30 percent of the total budget request.

The amount requested for training satisfies all OIG training needs for FY 2017.

C. Appropriations Table

The OIG FY 2017 budget plan is based on a level of effort for the two mission programs – Office of Audit and Office of Investigations. The table below shows the budget by program area for appropriation FY 2015, 2016, and 2017.

Resources Available for Obligation	FY 2015 Enacted		FY 2016 Estimated		FY 2017 Proposed	
	FTE	Amount (000's)	FTE	Amount (000's)	FTE	Amount (000's)
Appropriated Resources:						
Audit	424	$75,964	421	$77,433	427	$80,610
Investigations	724	$167,919	708	$171,167	720	$178,190
Total: Appropriated Resources	**1,133**	**$243,883**	**1129**	**$248,600**	**1147**	**$258,800**

*The FY 2017 total appropriated resources include the FTEs and funds requested for Cybersecurity.

Section 2 – Budget Adjustments and Appropriation Language

A. Budget Adjustments Table (in thousands)

Office of Inspector General	FY 2015 Enacted Level	FY 2016 Estimated Level	FY 2017 Proposed Level
FTE:	**1,133**	**1,129**	**1,147**
Object Classification:			
11.1 Full-time Permanent Positions	$142,661	$147,530	$150,230
11.3 Other than Full-time Permanent	$1,382	$563	$1,000
11.5 Other Personnel Compensation	$2,720	$2,252	$2,642
11.9 Total Personnel Compensation	**$146,763**	**$150,345**	**$153,872**
12.0 Personnel Benefits	$54,021	$55,542	$60,763
21.0 Travel	$6,772	$5,216	$6,484
22.0 Transportation of Things	$1,024	$708	$1,008
23.2 Rent Payments to Others	$6,202	$6,268	$6,711
23.3 Communications, Utilities, & Misc.	$1,957	$2,180	$2,218
24.0 Printing and Reproduction	$55	$47	$37
25.1 Advisory & Assistance Services	$16,102	$17,863	$16,468
25.2 Other Services (Goods / Services)	$140	$107	$785
25.3 Government Agencies	$203	$214	$200
25.4 Operation & Maintenance of Facilities	$69	$79	$89
25.6 Medical	$334	$335	$336
25.7 Operation and Maintenance of Equipment	$4,424	$5,673	$652
26.0 Supplies and Materials	$1,519	$808	$1,903
31.0 Equipment	$3,388	$3,215	$6,274
32.0 Lands and Structures	$910	$0	$1,000
Total Budget Authority	**$243,883**	**$248,600**	**$258,800**

B. Budget Increases and Decreases Descriptions

Chart of Significant Budget Changes	FY 2015 Enacted Level (*000's*)	FY 2016 Estimated Level (*000's*)	FY 2017 Requested Level (*000's*)	Net Change
11.0 through 12.0 Personnel Compensation & Benefits	$200,784	$205,887	$214,635	4% Net Increase $8,748

An additional $7 million is requested to support a complement level of 1,138 FTEs and to continue the current level of oversight to the Postal Service. Of this amount, $5 million is for anticipated increases for health benefits, salaries, and COLA and $2 million is required for the Office of Personnel Management mandated Federal Employees Retirement System (FERS) employer contribution percentage increases. In FY 2015, we absorbed an average of a 2% increase to the FERS employer contribution percentage and we anticipate absorbing an average of a 1% increase for FY 2016 as well.

The additional increase of $1.7 million is needed to support the additional nine positions which will bring us to a full complement of 1,147. The Claimant and Provider fraud initiative accounts for six positions and the Cybersecurity initiative accounts for three positions.

21.0 Travel	$6,772	$5,216	$6,484	24% Net Increase $1,268

The increase to Travel accounts for resuming travel to our FY 2015 level to support the requirements for the nine additional positions outlined above. In FY 2016, travel was reduced to allocate those funds to other critical needs.

23.2 **Rent Payments to Others**	$6,202	$6,268	$6,711	7% Net Increase $443

The increase to Rent Payments to Others accounts for the annual lease increase for office space. Most of our offices are located in Postal Service facilities to reduce costs.

25.1 **Advisory & Assistance Services**	$16,102	$17,863	$16,468	-8% Net Decrease -$1,395

The decrease to Advisory & Assistance results from shifting resources from contractors to FTEs. However, the budget was adjusted to include the $776,400 CIGIE assessment.

31.0 **Equipment**	$3,388	$3,215	$6,274	95% Net Increase $3,059

The increase to Equipment is needed to purchase software and technical equipment to ensure that OIG internal systems are protected from potential cybersecurity threats.

32.0 **Lands & Structures**	$910	$0	$1,000	Net Increase $1,000

The increase to Lands and Structures accounts for the number of capital projects needed in Postal space as we continue to align organization structure to Postal's in order to better meet their needs; therefore, increasing the number of building improvements/modifications required.

C. Reimbursable Authority

In FY 2017, reimbursable authority work to be performed is estimated at $500,000. The primary mission for the OIG reimbursable program is to develop partnerships with other government agencies to provide unique value added support to the Postal Service. The OIG intends to leverage its resources with these groups in order to share knowledge while meeting stated work requirements.

Other Resources: Offsetting Collections	**FY 2015 Actual (*000's*)**	**FY 2016 Proposed (*000's*)**	**FY 2017 Requested (*000's*)**
Offsetting Collections:			
Reimbursable Authority	$500	$500	$500
Total: Offsetting Collections	**$500**	**$500**	**$500**

D. Appropriation Language

Appropriation Language
Office of Inspector General **SALARIES AND EXPENSES** (Including Transfer of Funds) For necessary expenses of the Office of Inspector General in carrying out the provisions of the Inspector General Act of 1978, $258,800,000 to be derived by transfer from the Postal Service Fund and expended as authorized by section 603(b) (3) of the Postal Accountability and Enhancement Act (Public Law 109-435): *Provided that unobligated balances remaining in this account on October 1, 2016 shall be transferred back to the Postal Service Fund.*

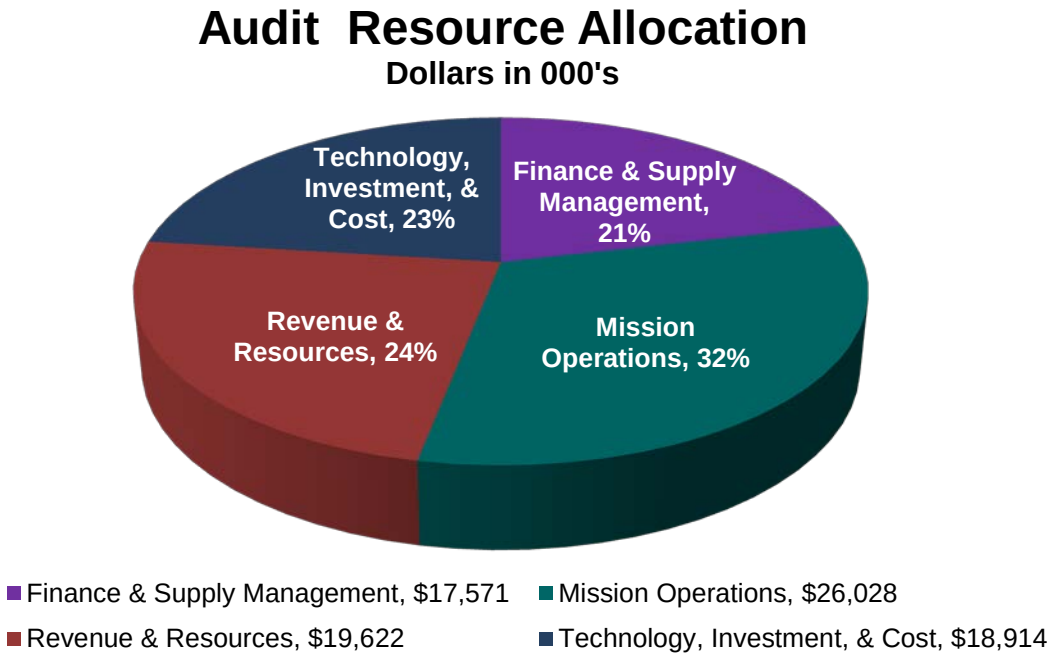
Section 3 – Budget and Performance Plan

A. Audit Budget and Performance Plan

The Office of Audit (OA) focuses on reviews that provide the Postal Service with information to address its emerging strategic issues, major risks, and management challenges. OA organizes its audit work to address risk factors in four functional audit areas — Mission Operations; Finance and Supply Management; Technology, Investment, and Cost; and Revenue and Resources.

OA has nine data analytic risk models which are critical in developing audit work and assessing operations and risks for the Postal Service. The models use risk factors and performance goals to gauge a program's performance, level of customer service, legal compliance, and internal controls. OA prepares and analyzes the risk models quarterly and shares the results with Postal Service stakeholders. This allows management and our audit staff to focus on specific program areas requiring further attention.

The following chart shows how OA would allocate its FY 2017 program budget of $82 million to the four functional audit areas. In FY 2015, OA identified $3.4 billion in monetary benefits a return on investment (ROI) of $44 for each dollar spent.



MISSION OPERATIONS: $26,028 Funds Requested

The Mission Operations audit area reviews the Postal Service's largest cost center functions — Network Processing, Transportation, and Delivery. The Postal Service delivered over 155 billion mailpieces in FY 2014 using its massive infrastructure, which includes over 488,000 full-time employees, 320 processing facilities, and over 35,600 retail and delivery units. In FY 2014, the Postal Service delivered mail to over 153 million residences and businesses each day.

Risk factors in these core functional areas are those that may impede the Postal Service's abilities to be effective and efficient in moving mail and to ensure service is maintained. Audit work that addresses the Mission Operations' objectives includes:

- Assessing delayed mail and the associated service implications
- Examining network rationalization of plants and other postal facilities
- Assessing overall efficiency of the processing and distribution networks
- Determining cost-effective opportunities for various transportation modes
- Identifying opportunities to reduce operating costs for rural and city delivery operations
- Benchmarking the Postal Service's operational processes against those of selected foreign posts and major corporations

The Mission Operations audit area performed 31 reviews and provided monetary benefits of over $176 million in FY 2015. Review highlights over the past 2 years include:

- Delivery operations reviews covering carrier efficiency, carriers returning after 5 p.m., vehicle fleet replacement and maintenance, additional carrier services, rural mail counts and timekeeping, parcel readiness, and vehicle parts inventory management
- Mail processing operations reviews covering plant consolidations, delayed mail, and parcel readiness
- Technology reviews covering parcel lockers, same day delivery, scanning, and the address management system
- Transportation operations reviews covering, transportation efficiency, postal vehicle services, surface visibility, mail transportation equipment service centers, highway contract route (HCR) efficiency, and capital property disposal

Over the past 2 years, audits in this area have concluded that the Postal Service should:

- Develop a comprehensive fleet management strategy which includes best practices of foreign posts
- Eliminate the Voyager card program and move to a fuel indexing supplier driven program
- Reduce delayed mail and refrain from making significant changes to the mail processing network, until the network stabilizes
- Eliminate workhours at inefficient plants and delivery units
- Reduce cost and improve efficiency in various transportation programs
- Update area mail processing data prior to consolidating facilities
- Innovate as necessary to meet emerging customer demands
- Update parcel technologies and systems to be more in line with the private sector

To best serve the Postal Service, Mission Operations will continue providing value-added audit reports and other products that focus on improving operations. This work will flow directly from several strategic focus areas the OIG has focused on, such as cutting costs, meeting emerging needs, improving customer service, and optimizing and modernizing operations.

The requested budget will allow us to:

- Perform audits focusing on cutting costs in areas that include, but are not limited to, efficiency, consolidation, carrier workforce, transportation, and vehicle reviews
- Conduct in-depth audits of the rural delivery program area, which costs over $6.6 billion annually, and the HCR program, which costs over $3 billion annually
- Perform audits that will bring the Postal Service in line with private industry on parcel handling and delivery, including upgrading package visibility technology
- Benchmark with foreign postal services to identify best practices and ideas for innovation and efficiency
- Conduct studies of Postal Service modernization, including considering outsourcing functions not associated with the core functional areas
- Identify best uses of network assets (logistics and delivery networks)
- Use data to channel our limited resources to areas most at risk and address emerging themes using data modeling and predictive analytics

- Focus on the emerging theme of modernization, with emphasis on updating the processing and delivery infrastructure, including carrier, vehicle, and parcel sorting equipment
- Inform the debate on major mission issues, including the closure of plants, service-level mandates, and modes of delivery

Furthermore, Mission Operations will increase the use of its data analytics risk models in audit planning and fieldwork. Mission Operations has developed various risk models and continues to refresh them and add new key risk indicators. In the past year, we have added an almost real-time delayed mail dashboard and other tripwires that we use on a daily basis to make audit decisions. The delayed mail dashboard and tripwire allowed us to implement a nationwide delayed mail strategy. We issued the first nationwide management alert on significant delayed mail as a result of service standard changes. This report addressed delayed mail systemically, rather than concentrating on a single plant. We also track spikes in delayed mail at the plant level, daily. This has allowed us to send quick response teams to the Maine and Colorado facilities, to identify causes and remedies for delayed mail in real time at those locations. We are currently automating our delayed mail reporting process, so we can expand coverage in this area.

As we continue to improve data analytics risk models, we will see cause and effect relationships across Postal Service operations, allowing OA to tackle larger problems and fix broad systemic issues. We have routinely used the models in all of our efficiency work involving plants, transportation, delivery units, and vehicles, which has allowed us to focus on the most severe problems.

FINANCE AND SUPPLY MANAGEMENT: $17,571 Funds Requested

The Finance and Supply Management audit area focuses on issues related to finance, contracting, and facilities management. These areas have a clear financial impact and support daily postal operations to optimize the supply chain and facilities operations and to help ensure accurate, accessible financial data and reporting. Cost control has been a primary (and critical) focus in these areas for the OIG and the Postal Service. Audit work that addresses Finance and Supply Management issues includes:

- Assessing financial reports and reporting controls
- Monitoring key financial activities and identifying cost saving opportunities to help ensure continued operations
- Evaluating the effectiveness of the facilities management and contracting strategies
- Reviewing supply chain and facilities costs to ensure they are adequately controlled by current policies, initiatives, and best practices

The Finance and Supply Management audit area performed 33 reviews and provided monetary benefits of nearly $374 million in FY 2015. In addition to these monetary benefits, Finance and Supply Management also provided the following outcomes over the past 2 years:

- Performed audits to assist the independent public accounting (IPA) firm in rendering its unqualified opinions on the Postal Service's financial statements and internal controls over financial reporting
- Identified ways the Postal Service could improve suspicious money order activity reporting in compliance with the Bank Secrecy Act
- Found additional ways to help the Postal Service ensure export controls compliance for international packages
- Evaluated controls around the highway contract route electronic payment process and oversight of purchase cards to ensure payments were proper
- Identified current technologies and strategies available for customer payment of parcels
- Evaluated assumptions used in the computation of and payments made towards significant Postal Service benefit liabilities (including pension, health care, and workers' compensation), showing that the Postal Service is closer to being fully funded, or potentially overfunded, for estimated liabilities when certain assumptions are reasonably adjusted or considered

- Assessed contracting practices related to professional service contract rates, delegations of authority, and use of a competition advocate to ensure the Postal Service was getting the best value out of its contracts
- Evaluated specific contracts and agreements to ensure the awards were proper and followed best practices
- Identified significant conflicts of interest with the firm that the Postal Service contracted with to negotiate property sales and lease transactions for the Postal Service

Over the past 2 years, audits in this area have concluded that the Postal Service should:

- Develop or remediate controls over point-of-sale software to improve revenue and operations, and decrease the risk of improper payments
- Educate Postal Service personnel on high risk money laundering activities and the importance of sharing information related to and reporting suspicious money order activity
- Use best practices, including data mining, to implement a continuous monitoring program over improper payments
- Revise and implement a plan to integrate Highway Contract Route tracking and payment technology in the Postal Service's payment process to reduce the risk of improper payments
- Rescind the delegation of authority to non-contracting personnel for service contracts
- Develop processes to ensure the contracting area's competition advocate is utilized by the Postal Service and effective in his or her duties to evaluate all applicable noncompetitive actions
- Reiterate to contracting officers the importance of collaborating with their internal business partners prior to solicitation to obtain clearly defined requirements

In order to best serve the Postal Service, the Finance and Supply Management audit area will continue to provide value-added audit reports and other products that focus on improving the financial control environment and address cost controls and savings. This work flows directly into the OIG's strategic focus areas related to cutting costs and recovering improper payments. Specifically, we will continue to work with Postal Service officials to identify risks and trends through the use of data analytics, financial control deficiencies, and supply chain best practices. This work will yield proactive recommendations that will help the Postal Service reduce its debt and costs, improve its liquidity, and implement processes to promote efficiency.

The requested budget will allow the Finance and Supply Management audit area to:

- Continue our annual support of the IPA firm's financial statement and internal controls opinions
- Provide opportunities and options to help the Postal Service improve its liquidity and assets and reduce its future liabilities
- Continue evaluating contracting practices associated with significant individual or Postal Service-wide contracts to ensure best practices are incorporated into Postal Service policies and processes
- Analyze Postal Service facilities to ensure they are adequately maintained, fully utilized and, as appropriate, disposed of in a manner that protects the interests of the Postal Service and stakeholders
- Upgrade our data analytics risk models to address some of the key financial (improper) payment, lease and contracting risks
- Continue to assess the Postal Service's efforts to generate revenue and reduce costs through facility optimization and opportunities to sell and lease properties

Data analytics risk modeling is essential to the success of the Finance and Supply Management audit area. We prepare and analyze multiple data analytics risk model results and share them with Postal Service stakeholders. These models are critical in developing audit work and assessing operations and risks for the Postal Service.

Examples of these models include:

- The Facilities data analytics risk model detects emerging risk that will permit OIG and Postal Service officials to more efficiently and effectively audit, investigate, and manage the Postal Service's real estate portfolio and optimization efforts. The model should help facilitate efforts to provide the best, least expensive facilities to support retail services and required mail processing and delivery operations. The model was used to identify lease cost savings of more than $2.2 million and $6.6 million in the Eastern Area and Northeast Area respectively.
- We are finalizing the development of a Supply Management risk model to identify areas that will increase the efficiency and effectiveness of the Postal Service's administration of contracts. We are also developing tripwires that will scan contracting data to identify anomalies (such as contracts older than 20 years).
- The Field Financial data analytics risk model assesses districts currently at risk from a financial standpoint (for example - local purchases, stamp stock inventory, revenue, and refunds) for potential audit and investigative attention.

Using the model data, we identified specific Postal Service locations with anomalies in their point-of-sale system data. As a result of audit work at those sites, we recommended the Postal Service implement or remediate controls over point of sale business transactions.

TECHNOLOGY, INVESTMENT, AND COST: $18,914 Funds Requested

The Technology, Investment, and Cost audit area focuses on issues related to financial and information systems. This area reviews the Postal Service's ability to use technology to manage operations, maximize return on investment and secure and protect existing technology. As technology is rapidly changing, the Technology, Investment, and Cost audit area evaluates governance, investment management, and protection of information resources and data used to support Postal Service operations. As a data rich organization, the Postal Service must continue to appropriately harness its data and use it to manage organizational performance. Our audit work will help the Postal Service design safeguards to minimize risk to systems, assets, and data.

Audit work that addresses Technology, Investment, and Cost issues includes:

- Best practices for using data to manage operations
- Processes for measuring and tracking performance of strategic initiatives and investments
- Evaluation of security and protection of sensitive data
- Vulnerability assessments to identify issues that may negatively impact the confidentiality, availability and integrity of systems
- Evaluation of system development, risk mitigation, and contingency planning
- Identification of controls to mitigate the risk of fraud
- Audits of selected major capital investments by the Postal Service of $5 million or more that focus on functionality and deployment
- Evaluation of compliance with the Postal Accountability and Enhancement Act (PAEA)

During FY 2014, the Technology, Investment, and Cost audit area developed the Project Management data analytics risk model. This model measures three basic indicators — program risk, program health and program budget — to identify system development activity that may be at risk. In addition, the Information Technology Security data analytics risk model measures security events such as spam and malware incidents that have occurred on Postal Service computers throughout the nation. These events can indicate whether a user is engaging in activity such as inappropriate web browsing, file exchanging, or email viewing — the three main conduits used to infect a network and disrupt system operations. The results of the risk model have led to six audit and five investigative referrals.

The Technology, Investment, and Cost audit area performed 25 reviews and provided monetary benefits of over $966 million in FY 2015.

Highlights over the past 2 years in the Technology, Investment, and Cost audit area include:

- Ensured accountability in Delivering Results, Innovation, Value, and Efficiency (DRIVE) initiatives via an audit and controls process for each project at the program manager level
- Reviewed decision analysis reports to ensure prudent capital investment
- Recommended management enhance controls over the Product Tracking and Reporting System to protect customer information
- Reviewed the Postal Service's management of cloud computing contracts
- Recommended improvements to the Postal Service's software development processes
- Recommended the Postal Service correct functionality issues in nationwide deployments of retail and delivery equipment
- Recommended the Postal Service develop a strategic plan to simplify package prices to reduce complexity for customers
- Recommended the Postal Service develop and execute a strong cybersecurity culture into daily operations through initiatives focused on security education, training, and awareness activities for all Postal Service employees, contractors, and senior leadership
- Recommended the Postal Service separate the joint duties of the chief information security officer and vice president of Digital Solutions and designate a senior-level chief information security officer with information security as the primary duty
- Recommended the Postal Service adequately staff cybersecurity operations based on the functions of the Security Operations Center and the Computer Incident Response Team

Over the past 2 years, audits in this area have concluded that the Postal Service should:

- Continue its initial cybersecurity initiatives while ensuring adequate resources and a coordinated proactive prevention, detection, response, and mitigation of sophisticated cyber threats is proactively implemented
- Ensure that their DRIVE and capital funding governance process is actively followed because it is used to measure and make business decisions about the most important Postal Service operational activities for closing the revenue gap
- Ensure accuracy of cost and pricing information to provide better pricing for customers

- Document cost and pricing information accurately for better operational data and decision making

Within this audit area, success is defined in terms of providing timely and relevant evaluation of Postal Service technology and use of data to stakeholders.

The requested budget will allow Technology, Investment, and Cost to:

- Identify potential security weaknesses within the Postal Service's computer applications and systems through vulnerability scanning and penetration testing
- Provide value-added audit reports and other products that focus on emerging technology and solutions, optimizing information technology programs, improving system performance and controls, and enhancing data security
- Assist the Postal Service in maintaining awareness of emerging technology and data needs
- Evaluate information technology strategies and governance programs
- Evaluate major capital investments to determine whether the deployment and functionality meets expectations
- Evaluate whether DRIVE initiatives follow best practices for closing the revenue gap in the Postal Service
- Review data collection systems and procedures used to prepare Annual Compliance Report (ACR) and ensure legislative compliance

REVENUE AND RESOURCES: $19,622 Funds Requested

The Revenue and Resources audit area focuses on issues related to Postal Service sales and marketing operations and human resource management, security, and emergency preparedness. This area also oversees the work at the Postal Inspection Service. Audit work in this area includes:

- Assessing the Postal Service's revenue generation and revenue protection strategies and processes
- Assisting the Postal Service in cost-effectively meeting its various legislative mandates
- Assessing the value of volume-based national service agreements
- Evaluating ways to reduce the Postal Service's Workers' Compensation Program cost
- Assessing the Postal Service's processes to ensure compliance with Occupational Safety and Health Administration (OSHA) regulations to protect employees and avoid OSHA penalties
- Overseeing investigative activities of the Postal Inspection Service

The Revenue and Resources audit area conducts a wide range of meaningful audit work promoting economy, efficiency, cost savings, integrity, and accountability. Our audits focus on revenue generation, human resource processes, employee costs, security of people and assets, and innovation at the Postal Service. We continuously solicit input from Postal Service management to determine their concerns and have built professional networks within both the Postal Service and the audit community to enhance our value and work. The Revenue and Resources audit area performed 32 reviews and provided a monetary benefit of $1.9 billion in FY 2015.

Over the past 2 years, audits in this area have concluded that the Postal Service should:

- Develop a city carrier compensation system based on time standards for specific tasks completed by a carrier, which would have resulted in savings of over $1 billion in FY 2015
- Improve controls over the Postal Inspection Service's Mail Covers program to ensure responsible personnel process mail covers in a timely manner and conduct periodic reviews of the mail covers program
- Improve controls to reduce employee and benefit costs, including supervisory, overtime, grievance and workers' compensation
- Strengthen the security clearance process to ensure contractors have the appropriate clearances

- Improve procedures to safeguard the mail and sensitive information and increase training to responsible personnel
- Implement best practices to decrease waste disposal costs and increase recycling revenue
- Improve the customer experience by providing quality service and developing expanded mailing and logistic options that meet the customer's needs
- Increase revenue by enhancing domestic and international sales and marketing efforts to all business and government mailers
- Offset the impact of low terminal dues rates by negotiating separate (bilateral) agreements with countries to exchange international mail at higher rates
- Explore opportunities, including potential legislative changes, that will allow it to diversify into the logistics marketplace, and ship and export in areas currently prohibited
- Improve the availability and use of seamless business mail acceptance and entry procedures

Data analytics risk models are essential to the success of the Revenue and Resources audit area. Our models are critical in developing audit work and assessing operations and risk for the Postal Service.

Examples of these models include:

- The Revenue Generation and Assurance Risk Model compares quarterly revenue to same period last year for commercial and retail channels at the national and district levels. This model identified $500 million in short-paid postage annually and is being used to identify specific products and locations with short-paid postage for further review.
- The Retail and Customer Service Risk Model monitors trends in retail revenue, which is revenue from retail window transactions, and alternate access revenue, which is revenue acquired through automated, online, consignment, phone, or mail. It also monitors trends in customer complaints. This model was used to identify poor performing offices from both a customer service and retail operations efficiency perspective. This model was also instrumental in providing data used to evaluate customer complaints handled by the Customer Care Centers.
- The Human Resources Risk Model contains seven metrics and was designed to detect emerging human resources related risk that can potentially impact employee morale, productivity, efficiency, and cost. Model results were instrumental in assisting with identifying facilities with excessive unscheduled leave and those with little unscheduled leave that were evaluated for best practices. Using the model data saved audit cycle time and related travel cost.

- Our Security Risk Model incorporates workplace violence data from Inspection Service cases, hotline complaints, grievances, and employee accidents. The model identifies selected areas of security risk at the area, district, and facility levels. It also facilitates audit work and related oversight activities. Using this model data, the audit team identified districts and facilities with the greatest occurrences of workplace violence and security incidents, which were instrumental in completing an audit on workplace violence.

The requested budget will allow Revenue and Resources to:

- Continue to provide value-added audit reports and other products that are forward-thinking and data driven
- Identify trends and make proactive recommendations that will help the Postal Service generate revenue, reduce employee costs, enhance security, and satisfy customers
- Advance our knowledge and skill sets with data analytics
- Provide opportunities for Revenue and Resources to cover broader areas
- Continue to conduct audits that will be nationwide in scope

Going forward, we will continue to build on our knowledge base and assess the Postal Service's opportunities to generate revenue and control costs. We will also continue to evaluate risks in the areas of revenue protection, human resources, security, emergency preparedness, and environmental sustainability.

Legislative Mandates

Almost $8.3 million of our OA budget is either legislatively mandated by Congress or directed to assist the Postal Service in meeting its legislative mandates. As indicated in the table below, the OIG spends over $2 million to oversee activities of the Postal Inspection Service and $765,868 to audit the data collection systems and procedures the Postal Service uses to prepare reports related to costs, revenues, rates, and quality of service for all products. The OIG also spends over $4 million to assist the Postal Service in meeting its legislative mandates by performing work such as audits supporting the public accountant's opinion on the Postal Service financial statements and compliance with Sarbanes-Oxley Act (SOX) and Securities and Exchange Commission (SEC) financial reporting requirements.

Legislative Mandates - Dollar Value by Identified Mandates		
Public Law Reference	**Mandate Description**	**Cost* *(000's)***
PL 109-435	Financial Statement/SOX Audit or Quarterly 10Q	$4,030
39 U.S.C. § 3652	Audits of Postal Service Data Collection Systems	$766
5 U.S.C. App. 3 § 8G(f)(2)	Oversight of the Postal Inspection Service	$2,045
Various	Audits in Support of Postal Service Mandates**	$1,431
Total Dollar Value		**$8,272**

*Based on FY 2015 audit work through September 30, 2015
** Although not legislatively mandated for the OIG, these financial and network optimization-related audits support legislative mandates for the Postal Service

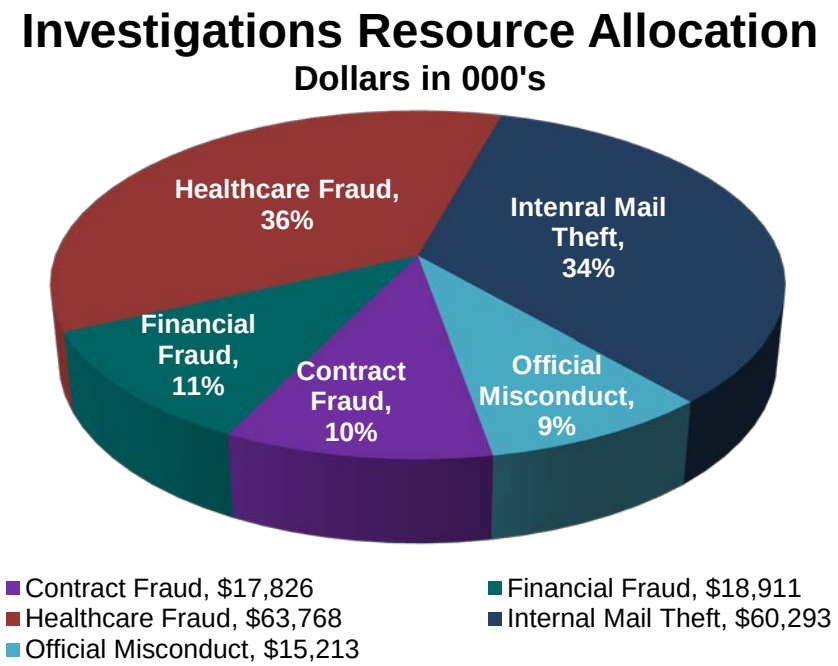
B. Investigations Budget and Performance Plan

The Office of Investigations (OI) performs work to protect the mail and to ensure the integrity of postal processes, finances and personnel. OI deploys its personnel in the field and headquarters based on the number of Postal employees, the need for specialized investigations, and Postal Service requested support. To facilitate planning and managing investigative work, OI field offices are aligned with Postal Area Offices allowing OI to focus efforts where there is the greatest potential for economic recovery. This alignment also enhances OI's responsiveness to the needs of the Postal Service.

To provide support for these investigations, OI organizes its work into five major investigative programs — Contract Fraud, Financial Fraud, Healthcare Fraud, Official Misconduct, and Internal Mail Theft. In addition to investigating the potential internal crimes and frauds listed above, special agents also investigate bribery, kickbacks, extortion, conflicts of interest, and allegations against postal executives. Furthermore, OI combats fraud and theft through crime prevention efforts.

The following chart shows how OI would allocate its FY 2017 program budget of $176 million to the five investigative programs. In FY 2015, OI identified $426 million in monetary benefits — a return on investment (ROI) of $3 for each dollar spent.

.



CONTRACT FRAUD: *$17,826 Funds Requested*

The Contract Fraud program aids the Postal Service by investigating allegations of contract fraud, waste, and misconduct. The Postal Service manages contracts, ranging from multimillion-dollar national contracts for services such as transportation networks and IT infrastructures to local contracts for supplies and services at individual postal facilities.

Investigative work that addresses Contract Fraud includes:

- Assessing risk of Postal Service acquisitions and contracts
- Investigating allegations of contract improprieties
- Documenting and presenting evidence for criminal and civil prosecution and administrative remedies

Below are some examples of our past and on-going casework that illustrate the impact we are making in combatting contract frauds.

- The Postal Service relies heavily on trucking companies to help move the mail and our OIG investigates those that commit fraud. Our agents investigated a company for overcharging the Postal Service for nearly $5 million in fuel as well as for committing Employee Retirement Income Security Act (ERISA) violations by stealing 401(k) funds. At one point, the company abandoned tractor trailers full of mail on the side of the road when it could no longer pay its employees' wages. The company, its owner, and its affiliates have been suspended and debarred, and prosecution is pending.
- The OIG also investigates allegations of kickbacks or bribes involving its managers. Our agents investigated two companies which bribed a station manager in return for steering additional work to their companies. The station manager also submitted false or inflated invoices to the Postal Service in return for a portion of the proceeds. The manager and owners of both companies were all convicted in Federal court and ordered to serve various prison sentences as well as pay restitution to the Postal Service.

In FY 2015, the Contract Fraud Program’s monetary benefit to the Postal Service was $75 million.

FINANCIAL FRAUD: *$18,911 Funds Requested*

The Financial Fraud program conducts two main types of investigations: embezzlement investigations and disbursement card investigations. A large portion of the revenue generated by the Postal Service is handled at the 31,000 postal retail locations.

Investigative work that addresses Financial Fraud includes:

- Investigating theft and misuse of Postal Service money and property
- Reviewing internal controls and identifying problems and solutions to prevent the loss of Postal revenues and assets
- Investigating and initiating administrative, civil, or criminal actions against individuals and firms responsible for the theft or misuse of Postal revenue and assets

Below is an example of our past casework that illustrates the impact we are making in the financial fraud program.

- The OIG investigated a Sales and Service Associate after receiving complaints of delayed deposits of remittances. Investigators determined that deposits had been consistently delayed for nearly 2 years. When agents interviewed the employee, she admitted to stealing over $230,000 in Postal funds. She explained that she stole the funds from remittance deposits and delayed submitting the deposits until she could pay for them with funds from the register. The employee was convicted in Federal court, sentenced to serve prison time, and ordered to pay full restitution to the Postal Service.

In FY 2015, the Financial Fraud Program's monetary benefit to the Postal Service was $4.4 million.

HEALTHCARE FRAUD: *$63,768 Funds Requested*

The Healthcare Fraud program conducts investigations for two main types of fraud: claimant fraud and medical provider fraud. Administered by the DOL, the Office of Workers' Compensation Programs (OWCP) provides direct compensation to providers, claimants, and beneficiaries. The Postal Service later reimburses the OWCP in a process known as "charge-back billings."

Investigative work that addresses Healthcare Fraud includes:

- Detecting and investigating allegations of fraudulent claims by individuals
- Detecting and investigating allegations of submitting false bills, colluding to extend benefits, and falsifying claim documents by medical providers

The government administers several healthcare programs for federal workers to ensure they receive medical treatment and potential wage compensation when they are sick or injured. For employees who suffer work-related injuries or illnesses, they receive compensation and medical benefits under the Federal Employees' Compensation Act (FECA), administered by the Department of Labor/Office of Workers' Compensation Programs (DOL/OWCP).

The Postal Service is the largest single contributor to OWCP and, in chargeback year 2014, it paid a total of $1.32 billion for FECA-related benefits. That same year, the Postal Service estimated its total liability for future workers' compensation costs to be $17.1 billion. These disability payments are funded by Postal customers rather than tax dollars and any portion of those funds lost to fraud by claimants or providers has a direct impact on the Postal Service and its customers.

The Claimant and Provider Fraud program at the Postal Service has consistently been a major focus for the OIG and has produced strong results. Each special agent has returned nearly $3 million in financial impact annually, in addition to the criminal and administrative outcomes associated with their work.

Below are some examples of our past and on-going casework that illustrate the impact our OIG is having in addressing healthcare fraud across government, particularly in the medical provider fraud area:

- We are a major contributor in the on-going investigation of a healthcare provider suspected of committing $500 million in fraud against the State of California and the DOL's OWCP. In 2014, the former owner of Pacific Hospital pled guilty to two charges related to this fraud and now faces up to 10 years in prison. In his plea agreement, he stated that he paid a State Senator bribes so the senator would support legislation that made the fraud scheme easier. The bribes included golf outings, private plane flights, and

expensive dinners. The Senator and a relative pled not guilty to charges of mail fraud, wire fraud, tax fraud, bribery, and money laundering.

- We were significant participants in some of the largest pharmaceutical investigations conducted in this country's history, including investigations of Pfizer (which paid $2.3 billion in criminal and civil fines), Novartis Pharmaceuticals Corporation (which paid $422.5 million in criminal and civil fines), GlaxoSmithKline (which paid $3 billion in criminal and civil fines), Abbott Laboratories (which paid $1.5 billion in criminal and civil fines), and most recently Janssen Pharmaceuticals (which paid $2.2 billion in criminal and civil fines). These completed investigations resulted in $9.4 billion in financial impact and our work resulted in the Postal Service receiving over $120 million of those proceeds.
- We led an investigation in Puerto Rico of two doctors and several claimants committing disability fraud. Undercover agents obtained recordings of the doctors as they falsified medical diagnoses and coached employees on what to say to DOL in order to receive disability benefits through OWCP. A Federal Grand Jury returned 12 separate indictments charging 10 current and former Postal employees and two doctors, with various healthcare frauds. Both doctors were convicted and sentenced to prison sentences and ordered to pay restitution. Some of the employees have been convicted and had their benefits reduced or terminated. The remaining employees are still in the litigation process and a determination of their benefits is on hold pending the end of litigation.

Because of our success, the Postal Service has encouraged the OIG for the past several years to shift additional resources to address these large threats. Since these task force cases require highly experience and capable special agents, as well as a long-term investment in investigative resources, the OIG needs to increase the number of tools and agents available to participate in these cases.

We propose to expand our Claimant and Provider Fraud program by an additional six positions to enhance our network of experienced claimant and provider fraud special agents across the seven major field offices and MFID.

In FY 2015, the Healthcare Fraud program's monetary benefit to the Postal Service was $345 million.

OFFICIAL MISCONDUCT: *$15,213 Funds Requested*

The Official Misconduct program is responsible for investigating misconduct by all postal employees and postal contractors. The OIG takes seriously any conduct by postal employees that deteriorates the public's trust and reflects negatively on the Postal Service. The Official Misconduct program investigates Postal employee misconduct including misuse of Postal Service computers, destruction or theft of Postal Service property, falsifying official documents, forgery, theft of funds, abuse of authority, sabotage of operations, and narcotics and alcohol abuse.

Investigative work that addresses Official Misconduct includes:

- Protecting the Postal Service and its customers from crimes and misconduct by postal employees and contractors
- Identifying and investigating general crimes and employee misconduct
- Assisting in prosecuting those responsible for official misconduct

Below is an example of our past casework that illustrates the impact we are making in the official misconduct area:

- In January 2014, the OIG learned that unclaimed packages from "Operation Santa" were addressed to a seasonal employee that had been assigned to work "Operation Santa". As background, this program is an annual letter-writing program for individuals, businesses and charitable organizations to respond to children's letters addressed to Santa Claus, the North Pole, and other seasonal characters. Agents eventually discovered that nine current and former employees were involved in two schemes to receive gifts from "Operation Santa". In the first scheme, the employees wrote their own letters and ensured those letters were selected by the Secret Santas. In the second scheme, the employees stole packages intended for underprivileged children by simply replacing the correct mailing address for the intended recipient with their own mailing addresses. In June 2015, three of the individuals were arrested and charged with conspiracy to commit mail fraud and receipt of stolen mail. Criminal charges are pending for the other six current and former employees.

The investigations in this program are designed to protect the public trust in the Postal Service and generally do not have large monetary benefits. In FY 2015, the Official Misconduct Program's monetary benefit to the Postal Service was $0.854 million.

INTERNAL MAIL THEFT: *$60,293 Funds Requested*

The Internal Mail Theft program investigates mail theft by postal employees and postal contractors. OI is responsible for investigating internal mail theft. The Postal Service depends on the public's confidence in the sanctity of the mail. The Postal Service and the public expect and demand a certain level of investigative service in this area.

Investigative work that addresses Internal Mail Theft includes:

- Protecting the Postal Service and its customers from mail delay, destruction, and theft
- Identifying and investigating allegations for theft, rifling, destruction, mistreatment, and obstruction of the mail
- Arresting and prosecuting those responsible for mail theft

Below are some examples of our past and on-going casework that illustrate the impact we are making in the mail theft program:

- A city carrier and his fiancée were arrested after investigators discovered an abandoned storage unit containing over 40,000 pieces of mail from the carrier's route. The storage unit was previously rented by the carrier's fiancée and the carrier later confessed to stealing and rifling this mail. During a search of the carrier's residence, investigators found a loaded AR-15 rifle, thousands of pieces of mail stacked up to the ceiling in one room, and two Neighborhood Delivery Collection Box Unit (NDCBU) parcel keys, which could access locked mailboxes. Both were convicted in Federal court and sentenced to serve prison time and pay restitution.
- After noticing increasing mail theft complaints along a particular carrier's route, agents investigated and ultimately arrested the carrier. When confronted, the carrier admitted to stealing mail for over a year. Prior to his arrest, agents discovered that he was routinely wearing body armor and carrying a firearm while on-duty and delivering the mail. The carrier was arrested without incident and prosecution is on-going.
- We arrested eight employees in New York who were systematically targeting suspected drug parcels and stealing them from the mail stream. The individuals were taking the parcels out of the facility through a rear door with its alarm disabled and video surveillance observed them take over 260 large parcels in a 3 month period. All eight were arrested and a number of them confessed to their participation in the scheme, a scheme which may have started almost 10 years ago according to one of the individuals. Prosecution is pending on all of the individuals.

Like the Official Misconduct programs, the investigations in this program are designed to protect the public trust in the Postal Service and generally do not have large monetary benefits. In FY 2015, the Internal Mail Theft Program's monetary benefit to the Postal Service was $0.478 million.

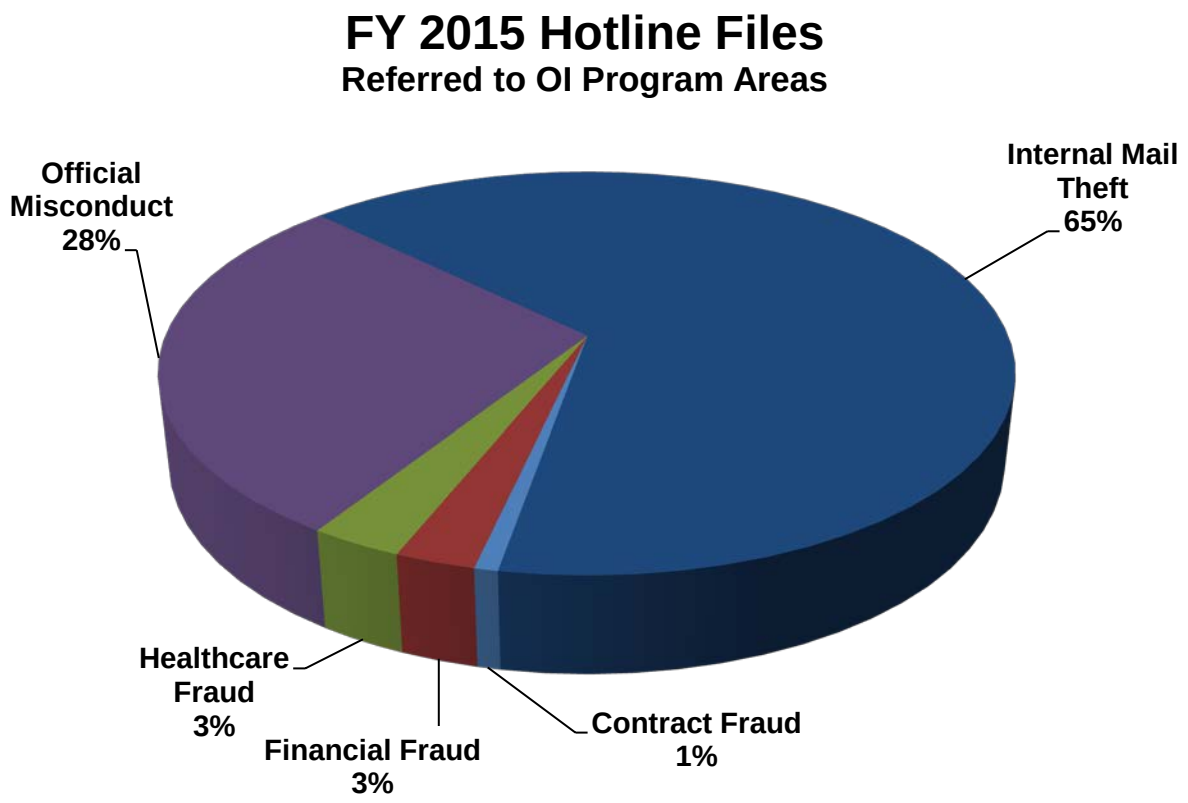
In FY 2017, OI plans to retain its focus on its five program areas and achieve financial results approximating $350 million, an increase of $85 million over the previous year's goals. These program areas show a large return on investment by identifying savings, which will assist the Postal Service in meeting future financial responsibilities.

HOTLINE CONTACTS

In FY 2015, 14,492 contacts for OI's five strategic program areas passed through the OIG hotline, making it an effective source of viable information to identify problem areas. As a result of investigations associated with these hotline contacts, the OIG has identified cost avoidance, fines, restitutions, and settlements.

The following chart shows the hotline volume by program area for FY 2015.

Program Area	FY 2015 Contacts
Contract Fraud	109
Financial Fraud	373
Healthcare Fraud	431
Official Misconduct	4,089
Internal Mail Theft	9,490
Total Annual OI Contacts	**14,492**
Other OIG Departments	2,909
Non-OIG Contacts	18,290
Total Annual Other Contacts	**21,199**
Grand Total Annual Contacts	**35,691**



C. Cybersecurity: *$654 Funds Requested*

The Cybersecurity program is a joint effort between OA and OI. Cybersecurity has drawn increasing attention in the past few years, as various government agencies and corporations have reported compromises to their networks. These compromises have resulted in millions of records being stolen for unknown purposes and the scale of the compromises continues to escalate. Often, the intruders were able to spend an extended period of time within the computer networks before being discovered, which have allowed them to analyze file systems and selectively steal the most valuable information.

The Postal Service has one of the largest computer networks in the world:

- The Postal Service network handles more than 13 million emails a day — more than 4 billion annually — delivered to nearly 211,000 email accounts. It scans 355 million internal email messages and more than 13 million external email messages for viruses every month. Nearly 103,000 email messages are blocked monthly due to viruses and more than 281,000 are blocked due to content.
- There are 3,473 remote locations within the postal system that receive Internet service via satellite.
- The network supports and maintains 125,000 desktop computers, 21,000 notebook computers, 85,000 printers, 11,000 cellphones, 152,000 phone lines and 310,857 handheld scanners.
- The Postal Service has 23 petabytes of storage capacity — equivalent to storing enough music to play continuously for more than 59,000 years.
- The Postal Service maintains 47,000 point of sale terminals nationwide and more than 340 million credit and debit card transactions are processed annually in Post Offices and through usps.com.

In September 2014, our OIG discovered that the Postal Service network had been seriously compromised. We led the initial investigative efforts to determine the scope of the compromise and assisted the Postal Service during its incident response and as it prepared a remediation plan. An assessment of the network's security infrastructure confirmed the poor state of the security environment and the monumental challenge in correcting those deficiencies.

In response to this growing focus on cybersecurity across government and the very real possibility that the Postal Service network remains vulnerable to future attacks, the OIG proposes to fill three positions in this area. This increase would support both the OI Computer Crimes Unit (CCU) and the Office of Audit's (OA) Information Technology Directorate (ITD).

OI's CCU would fill one position, which would include a cyber-investigator. OA's ITD would fill two positions, all of whom would be experienced cybersecurity IT specialists. These positions would allow OA to conduct vulnerability scanning and penetration testing as well as increase audit coverage of the Postal Service's cybersecurity environment within five key functional areas:

- Minimize risk to systems, assets, data, and capabilities
- Design safeguards to limit the impact of potential events on critical services and infrastructure
- Implement activities to identify the occurrence of a cybersecurity event
- Take appropriate action after learning of a security event
- Plan for resilience and the timely repair of compromised capabilities and services

Vulnerabilities are continuously being discovered and organizations must be constantly vigilant in identifying them and quickly remediating. The two most common techniques used for this purpose are vulnerability scanning and penetration testing. The Postal Service has already been receptive to vulnerability scanning, and has expressed interest in future penetration testing. Filling the positions within OA would enable the IT Directorate to obtain additional seasoned IT security professionals to routinely conduct this testing. Filling the positions within OI would enable the CCU Directorate to have expertise that would be embedded in critical locations within the Postal Service's IT security infrastructure allowing them to identify incidents sooner and respond faster to these compromises.

Section 4 – Supporting Materials

A. Human Capital Strategy Description

Description	FY 2015 Enacted Level	FY 2016 Estimated Level	FY 2017 Proposed Level
FTEs	1,133	1,129	1,147
Net Change from prior start of year to budget end of year	0	-4	+18

Due to the complexity of work within the OIG community, it is important to retain a highly specialized talent pool. We routinely examine the skills and knowledge needed by our professional staff and develop individual training plans to address identified skill gaps. Based on our leadership and succession plans, our mission requires training funds to build and maintain the analytical and technical skills of our workforce to address future performance outcomes, management goals, and leadership requirements. The number of experienced personnel the OIG can devote to these activities directly affects the length of time it takes to conduct complex reviews, audits, and investigations.

To that end, the OIG has undertaken a number of Human Capital initiatives to maintain our competitive edge. It is our commitment to build and maintain a highly engaged and talented workforce to achieve mission success, both now and in the future. We recognize that without a strong human capital strategy we cannot succeed as an organization unless we manage and invest in our workforce talent.

Our strategic human capital vision includes:

- Align workforce with the strategic priorities of the OIG
- Keep pace with our talent management strategy by implementing workforce planning capabilities, skills analysis, and other analysis tools
- Continue to identify OIG mission critical occupations and the core competencies associated with those occupations
- Develop employee mastery paths to include expert knowledge of:
    - Assignment
    - Profession
    - OIG operations

- Continue to build a robust succession planning program that aligns current talent development with future leadership needs
- Maintain an active, professional recruitment outreach function in order to effectively market the OIG to potential candidates
- Enhance the diversity of OIG's workforce by establishing partnerships with minority-serving organizations to help increase the pipeline of highly qualified minority applicants for OIG positions
- Develop communities of practices, instructor led training, and eLearning to maintain a continuous learning culture at all levels of the OIG
- Develop future leaders through structured management and leadership development programs; and leverage technology to support how we recruit, develop, and retain employees

Developing a strong Human Capital Strategy is vital to the OIG roadmap and path forward. With years of shrinking resources and the poor financial climate of the Postal Service, the OIG has turned toward hiring contractors to fulfill some of the IT support work, investigate workers' compensation issues, and to provide subject matter expertise. This necessary practice has allowed the OIG to keep pace with the IT community and meet users' needs for IT, increase positive investigative results concerning workers' compensation fraud and ensure current and best practices expertise in auditing Postal Services programs and operations. However, with the specialized nature of our OIG operations and an aging workforce, it is essential we invest in recruiting and retaining our own personnel to develop a bench of talent that has the capacity and bandwidth to contribute to the future successes as the Postal Service continues to undergo and experience significant change.

B. Information Technology Resources

Information Technology (IT) investment is critical to the OIG. It enables us to provide up-to-date technology that assures our auditors and investigators keep pace with and adapt to technological advancements in auditing, computer forensics, and IT security. The Office of Chief Information Officer (OCIO) integrates IT solutions that both allow for rapid response to the needs of the OIG and are adaptable to the constantly changing worldwide IT environment. The OCIO delivers purposeful solutions that leverage technology to accelerate the agency's innovation, capability, and efficiency.

The OCIO provides state-of-the-art capabilities to the core mission functions of auditing and investigating, regardless of geographical location. Funding for IT solutions enables the innovation required to research, develop, and deploy improved technology, and to enhance mission capabilities.

Examples include:

- Continuous improvements to organizational communication conduits, including data, voice, and video
- Integrating mobility solutions for broader OIG information accessibility
- Exploring hybrid cloud solutions technologies
- Strengthening the agency's cyber-security posture
- Providing and enhancing versatile and sophisticated applications
- Improving accessibility and security for mobile workforce via virtual desktop
- Focused, deliberate improvements in customer service for all products and value-added services
- Supporting rapidly evolving efforts in data analytics

Maintaining our IT infrastructure and IT security programs at an acceptable level requires continual upgrades to tools and technologies. IT funding provided to these program areas supports the data analytic efforts designed to enhance the effectiveness of investigators and auditors in a diverse and mobile environment. The funding also strengthens the security of our infrastructure, ensuring the information collected during audits and investigations of Postal Service operations and resources are not susceptible to cyber-attacks or other computer corruption.

During the past year, the OIG achieved its cost savings efforts through strategic IT investments. In keeping with the administration's FY 2017 budget guidance, the OIG continues to look for ways to reduce spending and to use our IT investment dollars more efficiently. The OCIO undertook many initiatives aimed at cost reduction and promoting a greener IT footprint. We leveraged the cost of our hardware, software

and operations. We also replaced outdated hardware and software technology with more efficient and effective computing platforms to improve IT accessibility and performance across our infrastructure (i.e., virtualization; cloud environment; energy efficient servers, monitors, and laptops; reduced data circuits; and lower telecommunications costs).

To strengthen the IT program's oversight, the OCIO continues to utilize the IT governance process to achieve greater integration with the Financial Investment Review Board. This strategy uses innovative technology to improve internal operations and integration with Postal Service systems to enhance operational efficiencies.

Information Technology Investments					
IT Investments / Funds Source ***(000's)***	**FY 2015 Enacted**	**FY 2016 Estimated**	**% Change from FY2015 to FY2016**	**FY 2017 Requested**	**% Change from FY2016 to FY2017**
Major IT Investments	$-	$-	$-	$-	$-
Non-Major IT Investments	$12,107	$12,349	2%	$12,596	2%
Infrastructure Investments	$-	$-	$-	$-	$-
Enterprise Architecture	$-	$-	$-	$-	$-
Total IT Investments	**$12,107**	**$12,349**	**2%**	**$12,596**	**2%**

Additionally, the OCIO ensured highly proficient, yet flexible IT capabilities for the OIG by employing a combined workforce of both federal employees and short-term contractors. This workforce combination enables the OIG to quickly flex necessary IT expertise when needed.

C. Predictive Analytics

Over the past 4 years, the OIG has developed and deployed several risk assessment tools that proactively identify vulnerabilities in several audit and investigative areas including contract fraud, mail theft, healthcare fraud, and financial fraud. The OIG continues to rely upon and invest in data analytics tools to focus our efforts on high-risk areas of the Postal Service and produce valuable work. As the technology used to transform raw data into meaningful and useful insights evolves, the use of predictive data analytics has become a necessary input into the OIG strategic goals and decision-making process.

In order to keep pace with the expanding amount of data and the rapid changes in data analytics capabilities, we are adopting new ways of conducting audits and investigations. More specifically, investments in innovative technology and tools such as text mining, which turns unstructured data into a more useful format and geospatial information system (GIS), which allows the ability to view, interpret, and visualize data to reveal relationships and patterns in the form of maps, have supported our mission. Implementing cutting-edge technology has assisted us with expanding capabilities to proactively analyze data, uncover trends, and decipher patterns to minimize financial risk, improve operational deficiencies, and prevent fraud exposure.

Combining disparate data sets and information into one place has assisted in improving efficiency. Our users access an interface that displays risk model results that is both intuitive as well as interactive allowing users the ability to drill down and export data (See Figure 3). By focusing our attention on high-risk fraud areas and schemes, we have helped shorten the investigative lifecycle. Data analytics has also helped us find the root causes of weaknesses in postal operations, and to offer solutions. In addition to having access to the fraud models, our auditors have access to risk models that provide insight on postal financial management as well as building and land leases.

The OIG performs approximately 535 recurring data extracts. Data is extracted from a wide variety of sources, including databases at the Postal Service, DOL, Social Security Administration, and OSHA. The extracted data supports numerous risk models, reports, tripwires, and other projects.

Our goal is to continue to develop increasingly valuable data mining models that transform data and information into shared knowledge. With the ongoing challenges the Postal Service faces, modernizing the OIG's capabilities to use innovative tools, technologies, and methodologies used to collect and analyze large volumes of complex information will help ensure that our work is of greatest value to the Postal Service.

The OIG will continue to incorporate the use of predictive data analytics as increasingly important tools for both detection and prevention of crimes in supporting our mission. Our OA efforts in FY 2015 resulted in 27 audits. These audits identified over $476 million in financial impact and $3.5 billion in non-financial impact. Our OI efforts in FY 2015 resulted in 734 investigations and/or cases opened and identified over $35 million in financial impact.

Our focus moving forward into FY 2017 is to enhance our current tools that support both our investigative and audit work.

Figure 3: Risk Model Results Sample