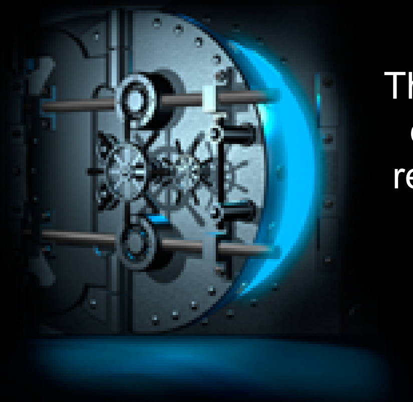


OFFICE OF
INSPECTOR
GENERAL
UNITED STATES POSTAL SERVICE

Security Risks in the Capital District

Management Advisory Report

January 27, 2014

Report Number HR-MA-14-003

OFFICE OF
INSPECTOR
GENERAL
UNITED STATES POSTAL SERVICE

HIGHLIGHTS

January 27, 2014

Security Risks in the Capital District

Report Number HR-MA-14-003

BACKGROUND:

The U.S. Postal Service's security program is designed to reduce the incidence of crime against employees, the mail, and other assets, as well as maintain the integrity of the Postal Service. The Postal Service faces a variety of security challenges and threats that it must take seriously.

Our objective was to determine whether the Capital District had an effective anonymous mail program in place to prevent potentially dangerous mail from entering the mailstream and a workplace violence program to mitigate violence.

We developed an enhanced security risk model to identify high-risk districts that warrant further review. We analyzed data related to anonymous mail, which is (b)(3):39 USC 410 (c)(2),(b)(7)(E) (b)(3):39 USC 410 (c)(2),(b)(7)(E) (b)(3):39 USC 410 (c)(2),(b)(7)(E) We also analyzed data related to workplace violence; suspicious and potentially dangerous mail; and Voice of the Employee survey results covering fiscal year 2012, Quarter 3, to fiscal year 2013, Quarter 2.

WHAT THE OIG FOUND:

The Capital District did not have an effective anonymous mail program in place to prevent potentially dangerous mail from entering the mailstream and a workplace violence program to mitigate violence. For example, the Capital District had an average anonymous mail testing failure rate of (b) percent. In addition, Capital District employees did not always follow policy when handling anonymous and potentially dangerous mail and did not always comply with workplace violence prevention requirements to effectively mitigate violence in the workplace.

The greatest opportunity to limit inappropriate use of the mail is during the earliest point in the Postal Service's distribution system. Potentially dangerous mail or an act of workplace violence could put employees, mail, assets, and the public at risk and negatively impact the Postal Service's brand. Enforcement of good security practices is essential to an efficient and economical operation.

WHAT THE OIG RECOMMENDED:

We recommended management clarify employee roles and responsibilities, require personnel to take additional training, implement anonymous mail program best practices, complete the workplace violence self-audit tool, and establish controls to ensure personnel comply with anonymous mail and workplace violence requirements.

Link to review the entire report

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

January 27, 2014

MEMORANDUM FOR: GUY J. COTTRELL
CHIEF POSTAL INSPECTOR

KELVIN L. WILLIAMS
DISTRICT MANAGER, CAPITAL DISTRICT

E-Signed by Michael A. Magalski
VERIFY authenticity with eSign Desktop

FROM: Michael A. Magalski
Deputy Assistant Inspector General
for Support Operations

SUBJECT: Management Advisory Report – Security Risks in the Capital District (Report Number HR-MA-14-003)

This report presents the results of our review of U.S. Postal Service security risks in the Capital District (Project Number 13YR001HR000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Andrea L. Deadwyler, deputy director, Human Resources and Support, or me at 703-248-2100.

Attachment

cc: Corporate Audit and Response Management

TABLE OF CONTENTS

Introduction

This report presents the results of our self-initiated review of U.S. Postal Service security data in the Capital District (Project Number 13YR001HR000). Our objective was to determine whether the Capital District had an effective anonymous mail[1] program to prevent anonymous and potentially dangerous mail from entering the mailstream and a workplace violence program to mitigate the potential for violence. See Appendix A for additional information about this review.

The chief postal inspector (CPI) is the chief security officer for the Postal Service and is responsible for developing and overseeing its security programs. The CPI assesses the security of the Postal Service's environment to ensure there is adequate protection. The Postal Service has a responsibility to provide a secure workplace, and all employees play a key role in each other's safety. Management must establish and maintain procedures, training programs, and communication channels to minimize potential threats. The Postal Service must be committed to ensuring a safe workplace for its employees, security for its transportation infrastructure, and safety of the general public.

We developed an enhanced security risk model to identify high-risk districts that warrant further review. Specifically, we obtained, reviewed, and analyzed data related to anonymous mail seeding[2] results, workplace violence incidents, and suspicious and potentially dangerous mail incidents covering Quarter (Q) 3, fiscal year (FY) 2012 to Q2, FY 2013. We incorporated Voice of the Employee[3] (VOE) personal safety and security survey responses. Additionally, we used the geographic information system (GIS) mapping portal to provide a visual tool for each of the security areas reviewed.

Conclusion

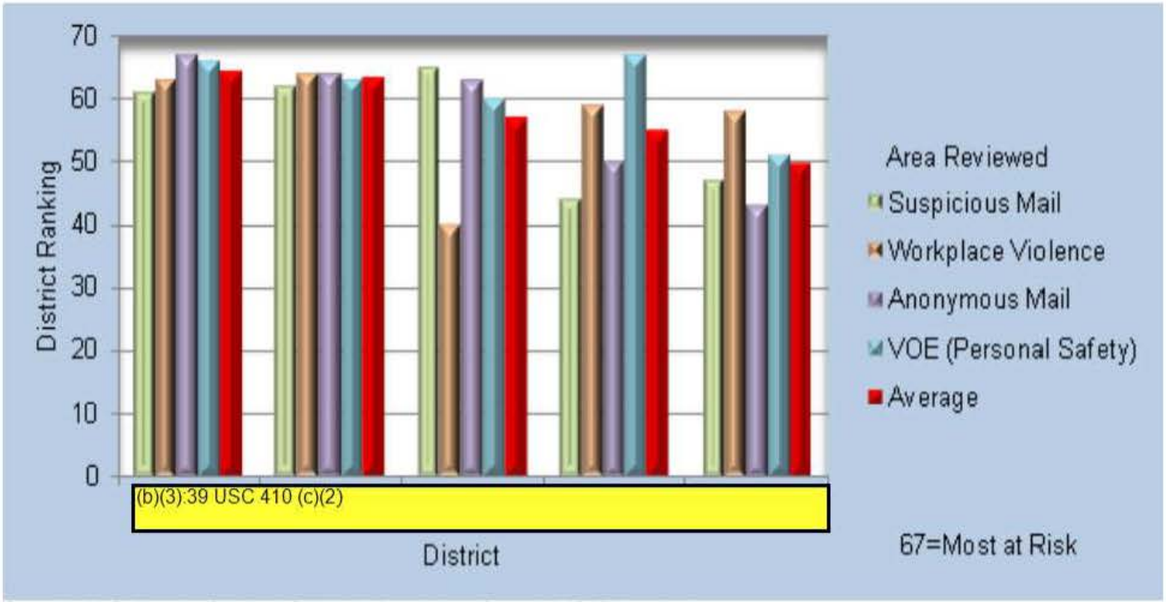
Of 67 districts, the Capital District ranked (b)(3):39 USC (see Figure 1). We found it did not have an effective anonymous mail program in place to prevent potentially dangerous mail from entering the mailstream and a workplace violence program to mitigate violence. For example, Capital District employees did not always follow policy when handling anonymous and potentially dangerous mail and did not always comply with workplace violence prevention requirements to effectively mitigate violence in the workplace. Potentially dangerous mail or a potential act of workplace violence puts employees, the mail, assets, and the public at risk. In addition, these types of incidents could negatively impact the Postal Service's brand; therefore, it is essential to maintain good security practices.

[1] (b)(3):39 USC 410 (c)(2),(b)(7)(E)
(b)(3):39 USC 410 (c)(2),(b)(7)(E)

[2] This testing is designed to study and measure the Postal Service's performance and success rate in adhering to protocols for handling anonymous mailpieces and effectiveness of the anonymous mail program.

[3] A periodic survey tool that assesses various workplace factors that can affect Postal Service employees, groups, and activities.

Figure 1: District Rankings from a Security Perspective: Top Five Most At-Risk Districts



Source: U.S. Postal Service Office of Inspector General (OIG) analysis.

Anonymous Mail

The purpose of the anonymous mail program is to prevent potentially dangerous mail from entering the mailstream and promote the safety of all Postal Service employees, customers, and transportation networks. (b)(3):39 USC 410 (c)(2),(b)(7)(E) (b)(3):39 USC 410 (c)(2),(b)(7)(E) (b)(3):39 USC 410 (c)(2),(b)(7)(E) All anonymous mail found in unattended locations or brought to a Postal Service facility by letter carriers or contract and delivery service providers should be (b)(3):39 USC 410 (c)(2),(b)(7)(E) (b)(3):39 USC 410 (c)(2),(b)(7)(E) An important aspect of the program is to monitor compliance with standard operating procedures.

Source: Postal Service.

(b)(3):39 USC 410 (c)(2),(b)(7)(E) (b)(3):39 USC 410 (c)(2),(b)(7)(E) Employees must recognize and properly handle anonymous mail to prevent potentially hazardous material from harming postal employees or being loaded onto commercial aircraft where it could harm passengers.[4]

[4] There are about (b) explosive devices per (b) billion mailpieces.

We analyzed anonymous mail (b)(3):39 USC 410 (c)(2),(b) from Q3, FY 2012 to Q2, FY 2013 and ranked districts based on failure (see Appendix B for anonymous mail district rankings and their average failure rates). With an average failure rate of (b) percent over the last 4 quarters, the Capital District ranked (b)(3):39 USC out of 67 districts (see Figure 2). The median failure rate for districts in the Capital Metro Area is (b) percent.

Figure 2: Capital Metro Area – Anonymous Mail (b)(3):39 USC 410 (c)(2), (b)(7)(E) Percentages

(b)(3):39 USC 410 (c)(2),(b)(7)(E)

Source: OIG analysis.

The Anonymous Mail (b)(3):39 USC 410 (c) map illustrates (b)(3):39 USC 410 (c) results for the Capital District (see Figure 3). (b)(3):39 USC 410 (c) (2) seedings conducted in the Capital District failed. The map also separates geographic areas of responsibility according to each manager, Post Office Operations[5] (MPOO). For example, the most failures occurred in the MPOO 1 area with (b)(3):39 USC 410 (c)(2),(b)(7)(E) In addition, the other three MPOO areas had (b)(3):39 percent failure rates. Based on what the map shows, the district manager could isolate and focus on incidents more easily in a specific MPOO area and take corrective actions as necessary.

Figure 3: Anonymous Mail (b)(3):39 USC 410 (c)(Map

(b)(3):39 USC 410 (c)(2),(b)(7)(E)

Source: OIG analysis.

[5] A manager in the district who has oversight of many associate Post Office facilities.

Anonymous Mail Handling

Capital District employees did not always follow policy when handling anonymous and potentially dangerous mail. Specifically, the Capital District had a (b) -percent failure rate regarding anonymous mail (b)(3):39 USC over the 4 quarters we reviewed. This occurred because employees were not properly trained and management did not provide sufficient oversight and hold employees accountable for detecting and preventing anonymous and potentially dangerous mail from entering the mailstream. Additionally, homeland security coordinator[6] (HSC) roles and responsibilities for follow-up testing and training were not consistent. As a result, the Capital District is at a high risk of allowing potentially dangerous mail to enter the mailstream undetected.

(b)(3):39 USC 410 (c)(2) employees we interviewed were either unaware of or not completely aware of Postal Service policies for handling anonymous and potentially dangerous mail. We reviewed the training records for (b) Postal Service employees at the facilities visited and found that none had completed anonymous mail training nor had they received stand-up talks related to anonymous mail (see Appendix C for list of facilities we reviewed).

Postal facilities that consistently fail to recognize anonymous mail or handle it properly must be identified and reported to the HSC to allow for additional testing and training of responsible personnel. Additionally, Postal Service area and district personnel must ensure that local follow-up testing is conducted with the assistance of the HSC at problem facilities, but it is unclear who is supposed to conduct it. For example, the Capital District HSC stated that facility managers are responsible for the additional testing and training, while the Nevada-Sierra District HSC stated that he conducts the additional testing and training as necessary to ensure compliance. Further, Postal Inspection Service officials stated that they are considering a more structured approach to the HSC role to ensure nationwide consistency and improve anonymous mail program compliance.

Additionally, we reviewed anonymous mail practices in the Nevada-Sierra District, which ranked (b)(3):39 USC on anonymous mail (b)(3):39 results, and found they had tools and processes in place that could enhance the Capital District's compliance. The acting district manager for the Nevada-Sierra District stated that they have taken action in conjunction with the HSC to improve anonymous mail compliance, including:

- Implementing an anonymous mail certification program that requires facilities to certify that management has provided stand-up talks to employees.
- Increasing the frequency of anonymous mail training and stand-up talks that incorporate simulations of the anonymous mail process.

[6] Postal Inspection Service personnel responsible for overseeing and monitoring anonymous mail program compliance.

- Conducting follow-up (b)(3):39 USC 410 (c)(2),(b)(7)(E) at failed facilities to address noncompliance with anonymous mail requirements.

- Sending operations support staff to facilities to watch the end-of-day, close-out process to ensure anonymous mail is handled properly.

- Ordering anonymous mail awareness stickers for placement in blue collection boxes beginning in FY 2014.

According to the Nevada-Sierra acting district manager, the anonymous mail failure rate has decreased as a result of the additional changes implemented.

Workplace Violence

The Postal Service has long recognized the importance of ensuring the safety of its employees by creating and maintaining a violence-free work environment. In addition, the Occupational Safety and Health Administration requires the agency to provide a safe and healthy working environment for its workers. Workplace violence[7] can occur at or outside the workplace and can range from threats and verbal abuse to physical assaults and homicide. Workplace violence is a growing concern for employers and employees nationwide and is one of the leading causes of job-related deaths.

Source: Postal Service.

Workplace violence can strike anywhere and about 2 million American workers are victims of workplace violence each year. Some workers, however, are at increased risk, including letter carriers. The most effective way to respond to the problem of workplace violence is to establish preventative measures. An established workplace violence prevention program provides the foundation for achieving a violence-free workplace. Such a program depends on a universal zero tolerance policy statement and a consistently implemented zero tolerance action plan for managing threats and assaults.

Quantifying the acts and means of violence is limited to a numerical measure of the problem, but numbers cannot convey the meaning of loss of a human life, the emotional impact on those affected, and the qualitative cost to society. Violence increases stress, inflicts emotional wounds, and lowers morale. Organizationally, it diminishes credibility, decreases productivity, creates work-specific tension, and sometimes has a significant financial impact as well.

A major component of the Postal Service's workplace violence prevention program is the threat assessment team (TAT). Capital District TAT members are trained to assess the danger or harm of threats – implied or direct – to victims. The team's goals are to

[7] Violence or the threat of violence against workers.

reduce risks to employees and the Postal Service, discourage inappropriate behavior, and resolve conflicts.

We analyzed workplace violence incidents from Q3, FY 2012 to Q2, FY 2013 and ranked districts based on the number of incidents reported compared to the employee complement. Of 67 districts, the Capital District ranked as the 5th most at risk and ranked higher than other districts in the Capital Metro Area. It is critical that the Capital District ensure employees understand that reported claims of workplace violence will be investigated and remedied promptly. For example, on September 18, 2012, postal inspectors and postal police responded to a letter carrier being physically assaulted by a customer while on his delivery route in Oxon Hill, MD. The carrier was transported to the hospital with unknown injuries, and a suspect was arrested and is in custody.

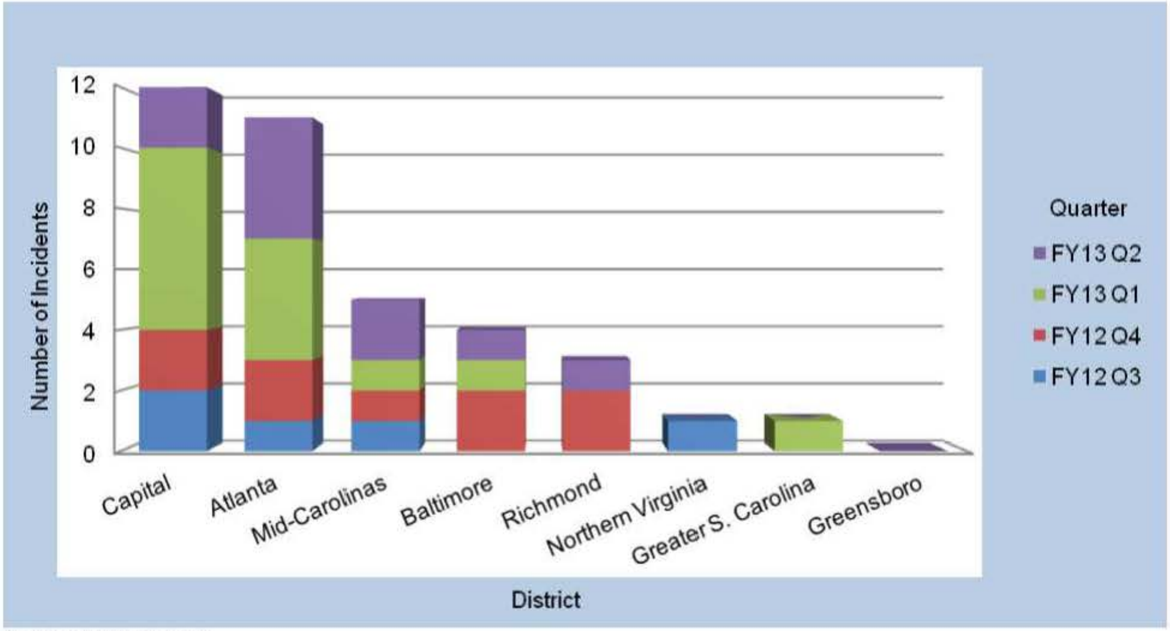
The Capital District reported 12[8] workplace violence incidents to the Postal Inspection Service over the last 4 quarters (see Figure 4). In addition, we identified grievances[9] in the Capital District over the same period involving assaults,[10] threats[11] or battery.[12] According to the Capital District manager, there were significantly more than 12 workplace violence incidents; however, district officials could not identify how many additional incidents were handled internally and not reported to the Postal Inspection Service.

Postal Service officials developed a Workplace Environment Tracking System (WETS) to track workplace violence incidents and launched it in August 2013. The purpose of WETS is to create a nationwide repository for initial management inquiries, workplace harassment fact-finding investigations, TAT cases, and workplace environment interventions. In addition, WETS will enable the Postal Service to enforce protocols and analyze data to identify trends and preventative measures regarding workplace harassment, threats, assaults, and overall workplace environment issues.

We also included Washington, D.C. crime statistics to enhance employee awareness regarding various crimes occurring in parts of the Capital District (see Appendix D for additional information on criminal activity in this district). Overall, total crime has increased by 1 percent over the last 2 fiscal years, but some types of crime have increased by a significantly larger percentage. For example, sex abuse has increased by 43 percent; and robberies, assaults, and thefts have also increased. Awareness of local crime statistics may help employees better understand crime and violence trends in their areas and take safeguards as appropriate.

[8] There were four robberies, seven assaults or threats, and a vehicle shooting.
[9] A dispute, difference, disagreement or complaint between the parties related to conditions of employment.
[10] Any willful attempt to inflict injury on another person.
[11] A statement or act intended to inflict harm or injury on another person.
[12] The use of force against another person involving harmful or offensive physical contact.

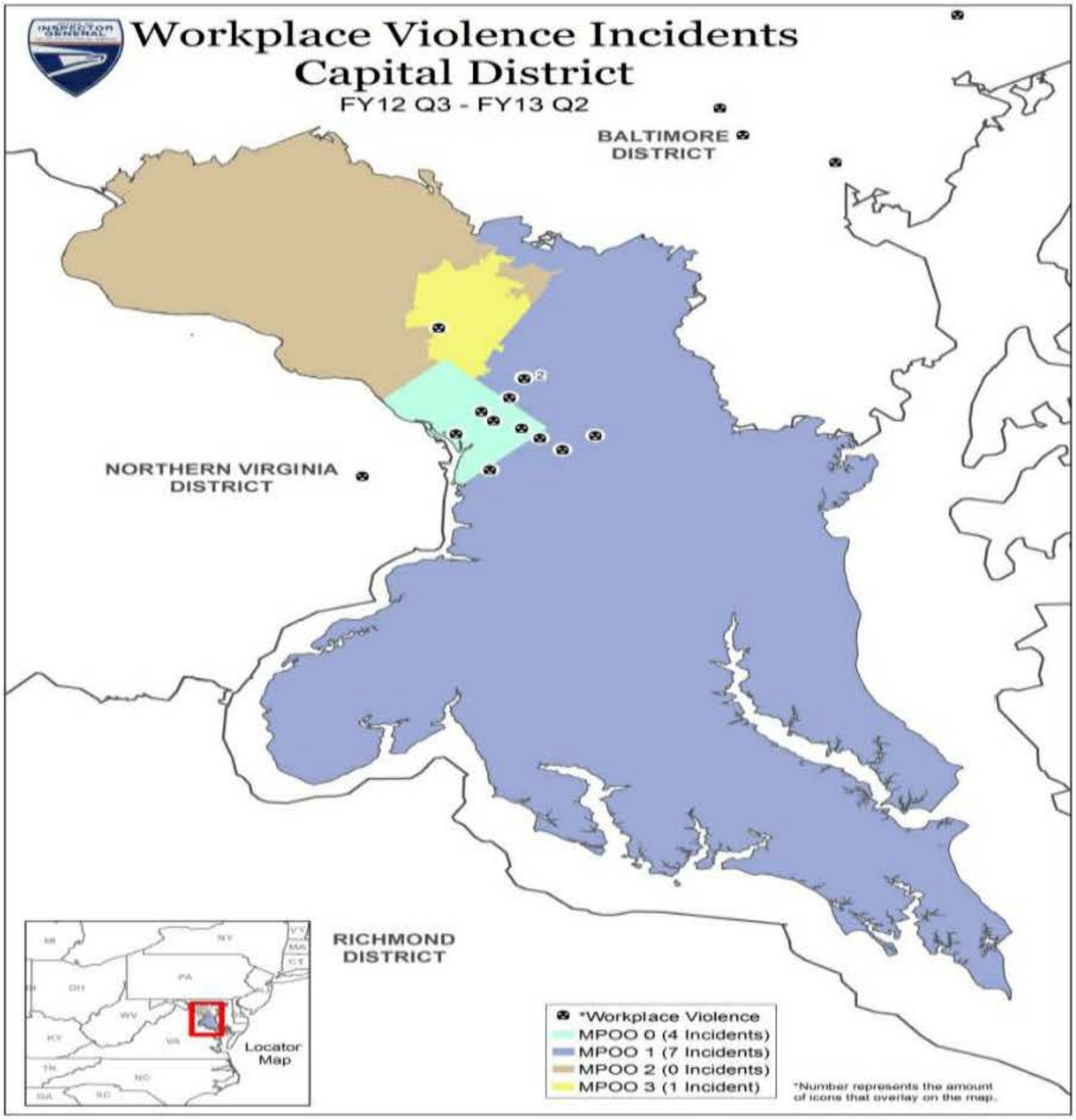
Figure 4: Capital Metro Area – Workplace Violence Incidents



Source: OIG analysis.

The Workplace Violence Incidents map shows incidents that were reported to the Postal Inspection Service's Headquarters Watch Desk (see Figure 5).[13] The map also separates areas of responsibility according to MPOO. The area identified as MPOO 1 had seven reported incidents, while MPOO 2 did not have any incidents.

Figure 5: Workplace Violence Incidents Map



Source: OIG analysis.

[13] The Postal Inspection Service's Headquarters Watch Desk receives information about critical events that may have national implications and require immediate action.

Workplace Violence Prevention

The Capital District did not always comply with workplace violence prevention requirements to effectively mitigate violence in the workplace. Specifically, the TAT did not identify core members, track workplace violence incidents, conduct quarterly meetings, or conduct post-incident analysis on all workplace violence cases ranked priority 1[14] and priority 2,[15] as required. This occurred because TAT members did not always receive required training[16] and complete the annual self-audit tool.[17] In addition, management did not provide sufficient oversight to ensure workplace violence incidents were handled appropriately. For example, management did not have sufficient controls in place to ensure the TAT complied with workplace violence policies and procedures. As a result, there is an increased risk that the TAT will not achieve its primary mission of preventing and mitigating workplace violence.

One of the first steps in establishing a TAT is to identify core members. We requested a current list of core TAT members from management but received multiple conflicting lists. For example, some of the core TAT members on the lists were no longer part of the TAT and some were supposed to be on the lists but their names were missing. We also requested the Human Resources manager provide documentation related to the total number of workplace violence incidents, quarterly TAT meetings, and post-incident analysis but determined the information was not complete or did not exist.

[14] A clear and immediate threat of violence to an identifiable target.

[15] A threat of violence, usually to an identifiable target but currently lacking immediacy and/or a specific plan or a specified plan of violence but currently lacking a specific target.

[16] Five of six employees listed as core TAT members did not complete the required workplace violence training.

[17] A workplace violence prevention compliance checklist completed during Q4 of each fiscal year to ensure TATs have identified core members, received training, conducted quarterly meetings, and are adhering to other workplace violence policies and procedures.

Suspicious Mail

The Postal Service safely delivers billions of letters and packages each year; however, its employees report only a small number of mailpieces as suspicious or containing suspicious substances.[18] The purpose of the Postal Inspection Service's Dangerous Mail Investigations program is to protect the Postal Service, its employees and customers, and the nation's mail system from criminal attack or misuse. After anthrax in the mail took five lives and harmed others in 2001 and incidents such as ricin mailings and panic-causing hoaxes and threats escalate, the Postal Inspection Service has stepped up its responses to mail-related terrorism and hazardous material. In addition, management and employees are required to undergo periodic training on suspicious mail[19] and unknown substances response procedures and managers and supervisors must ensure that employees follow those procedures.

Source: Postal Inspection Service.

For more than 200 years, postal inspectors have investigated bombs, poisons, and other dangerous items in the mail. Teams of postal inspectors are trained to respond to chemical, biological, radiological, and explosive incidents involving the mail and, in concert with other "first responders," use their unique knowledge of the mail and postal systems to identify and preserve evidence for criminal investigation. Postal inspectors are integral to the development and deployment of equipment that detects biohazards in the mail. Postal inspectors provide security guidelines and on-site evaluations to help identify security risks and educate businesses on safe mail handling.

We analyzed suspicious mail data from Q3, FY 2012 to Q2, FY 2013 and ranked districts based on the number of incidents reported compared to mail volume. Of 67 districts, the Capital District ranked the (b)(3) most at risk. While it is difficult to conclude what risks are associated with this ranking, management can use this information to identify anomalies and analyze trends. Management can also follow up on individual incidents to obtain more information on handling and response. When suspicious mail is reported, additional attention and response is required to ensure its safe handling. Although most reported suspicious mail incidents are determined to be nonhazardous, a small number of dangerous mailpieces have gone through the postal system, such as the ricin letters in April and May 2013. The Capital District must continue to be vigilant in identifying and isolating potentially dangerous mail.

The Capital District reported (b)[20] suspicious mail incidents over the last 4 quarters, which is higher than any other district in the Capital Metro Area (see Figure 6). Postal

[18] Suspicious substances are sometimes found loose in the mailstream and cannot be attributed to a specific mailpiece. Employees should follow the same protocols they would if a specific mailpiece was involved.
[19] Suspicious mail typically falls into one of the following categories: mail leaking suspicious powders; mail leaking suspicious liquids; mail containing suspicious items; mail displaying the threat of hazardous content; and emergency situations involving mail emitting smoke, fumes, or vapors.

Inspection Service and Postal Service officials stated that the higher number of incidents could be due to vigilant employees identifying and isolating suspicious mail. The ricin and anthrax incidents occurred in the Capital District where employees are responsible for handling mail for about 280 federal agencies. In addition, Postal Service management stated they recommend reporting anything that seems suspicious, including mail, liquids, odors, and powders.

Figure 6: Capital Metro Area – Suspicious Mail Incidents

(b)(3):39 USC 410 (c)(2)

Source: OIG analysis.

[20] (b)(3):39 USC 410 (c)(2)
(b)(3):39 USC 410 (c)(2)

The Suspicious Mail Incidents map illustrates the total reported incidents for the Capital District (see Figure 7). The map also separates areas of responsibility according to MPOO. The MPOO 0 Area accounted for [redacted] percent of reported suspicious mail incidents in the Capital District.

Figure 7: Suspicious Mail Incidents Map

(b)(3):39 USC 410 (c)(2)

[redacted]

Source: OIG analysis.

Voice of the Employee

Source: Postal Service.

The Postal Service tracks employee engagement through one of the largest employee opinion surveys in the nation. Since 1999 the Postal Service has administered the VOE survey to a sample of employees each quarter. The survey gathers confidential, voluntary, and on-the-clock responses to a series of questions related to one's job and work environment. The survey is an important instrument for measuring employee engagement in the Postal Service.

Engagement is the extent to which people enjoy and believe in what they do and how valued they feel for doing it. It is a positive attitude held by the employee toward the organization and its values that influences employees to invest and spend discretionary effort to help the organization succeed. High levels of employee engagement drive desirable organizational outcomes such as customer satisfaction, productivity, safety, and retention.

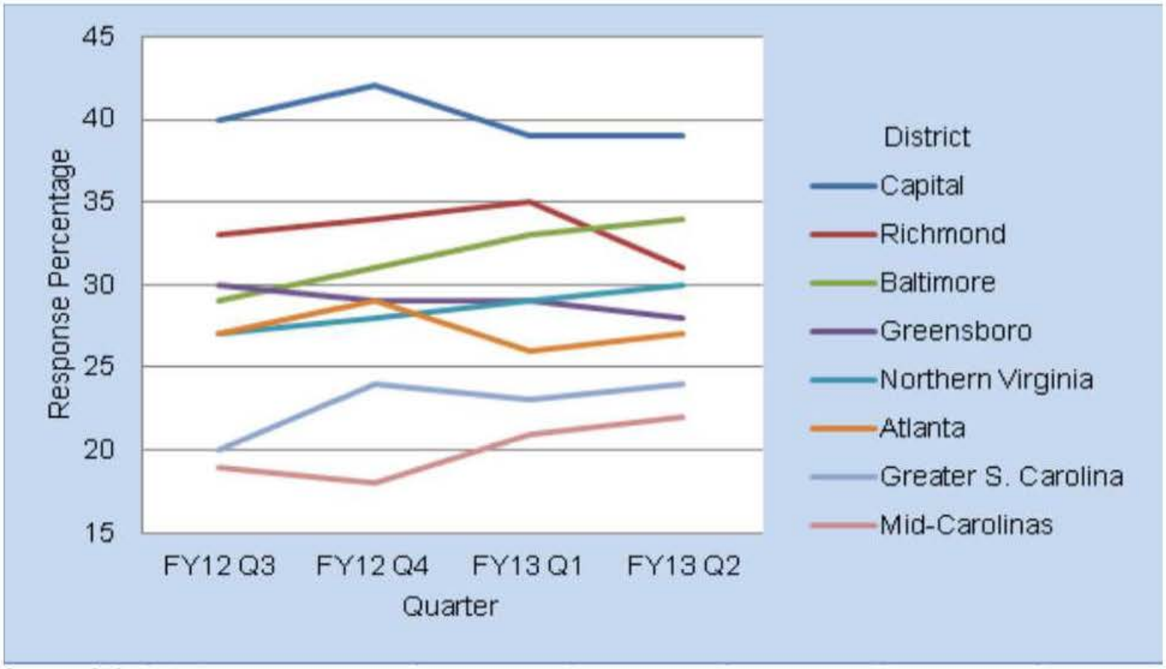
We analyzed VOE survey results from Q3, FY 2012 to Q2, FY 2013 and ranked districts based on neutral and unfavorable survey responses to the following four statements we identified related to personal safety and security:

- I am aware of the security measures in my workplace.
- I receive information to perform my job safely.
- Rate the physical working conditions.
- I feel safe from physical harm at work.

The Capital District had an average of 59 percent neutral or unfavorable responses related to rating the physical working conditions. The rest of the statements received an average of 33 to 40 percent neutral or unfavorable responses.

Of 67 districts, the Capital District ranked the 2nd most at risk and had an average of 40 percent neutral or unfavorable responses related to safety over the last 4 quarters (see Figure 8). According to the results, some employees in the Capital District do not appear to have a favorable outlook regarding safety and security in the workplace. Postal Service officials stated the results could be from a particular area in the district where a previous incident occurred or from an area where there is higher criminal activity. In addition, employees may begin to feel unsafe when they hear about drivers being robbed or other violent incidents. As a result, opportunities may exist for the Capital District to improve employee engagement regarding safety and security.

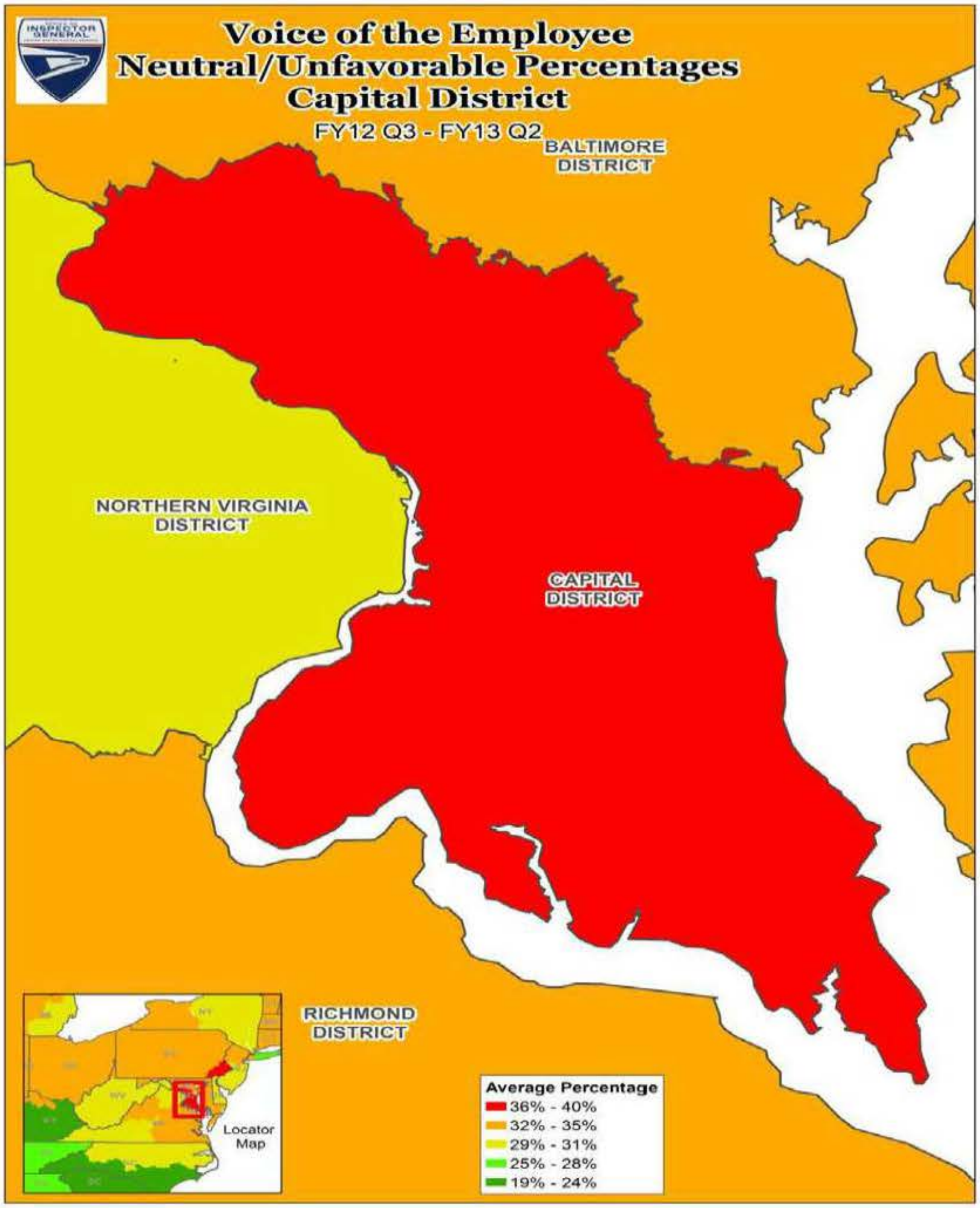
Figure 8: Capital Metro Area – VOE Neutral/Unfavorable Response Percentages



Source: OIG analysis.

The VOE map shows neutral and unfavorable survey responses based on four personal safety questions for the Capital District and surrounding districts (see Figure 9).

Figure 9: VOE Neutral/Unfavorable Percentages Map



Source: OIG analysis.

Geographic Information System Mapping

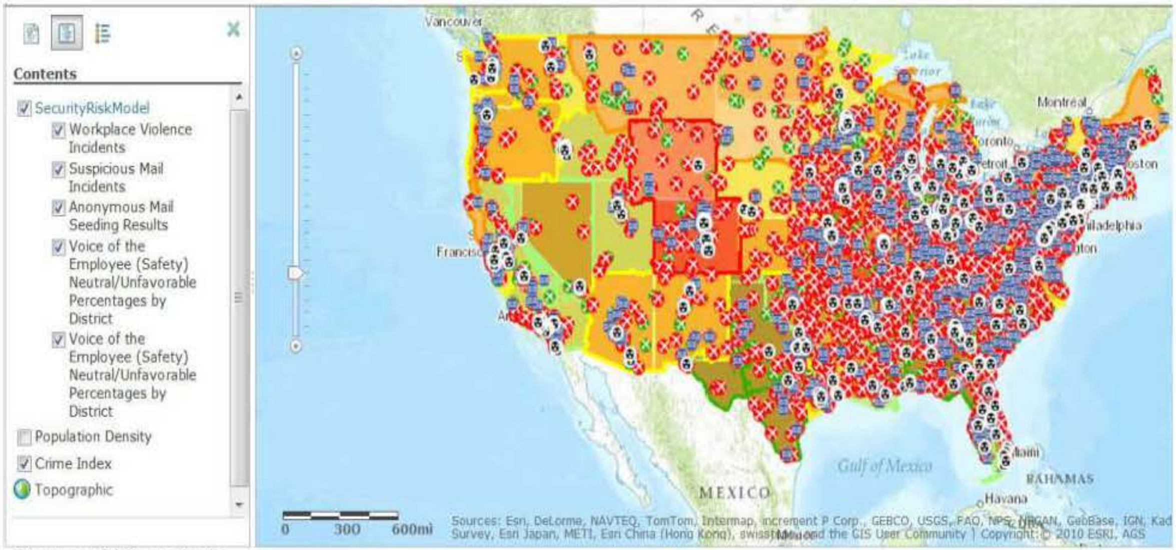
The GIS mapping portal is an online central storing system that allows users to access a variety of maps, data, and applications. Currently, the portal is only available to the OIG internally, but efforts are underway to make it accessible to other stakeholders.[21] By using the portal, users can incorporate various data to provide valuable insight into security-related events in the Capital District. The user can visually identify broad security trends or drill down to specific areas, districts, or cities and view details pertaining to each location. In addition, the portal allows filtering that can enable the user to view only certain types of incidents or data.

As part of our mapping analysis, we incorporated security and other data including the following:

- FBI crime statistics by type for cities with a population of 100,000 or more.
- Color-coded crime index.
- Color-coded population index.
- Color-coded VOE neutral/unfavorable results by district.[22]
- Suspicious mail incidents.
- Workplace violence incidents.
- Anonymous mail seeding results.

We incorporated the following examples that include various types of views with drill-down capabilities to specific neighborhoods and streets (see Figures 10-14).

Figure 10: Security Areas Reviewed



Contents

☑ SecurityRiskModel
- ☑ Workplace Violence Incidents
- ☑ Suspicious Mail Incidents
- ☑ Anonymous Mail Seeding Results
- ☑ Voice of the Employee (Safety) Neutral/Unfavorable Percentages by District
- ☑ Voice of the Employee (Safety) Neutral/Unfavorable Percentages by District

☐ Population Density

☑ Crime Index

Topographic

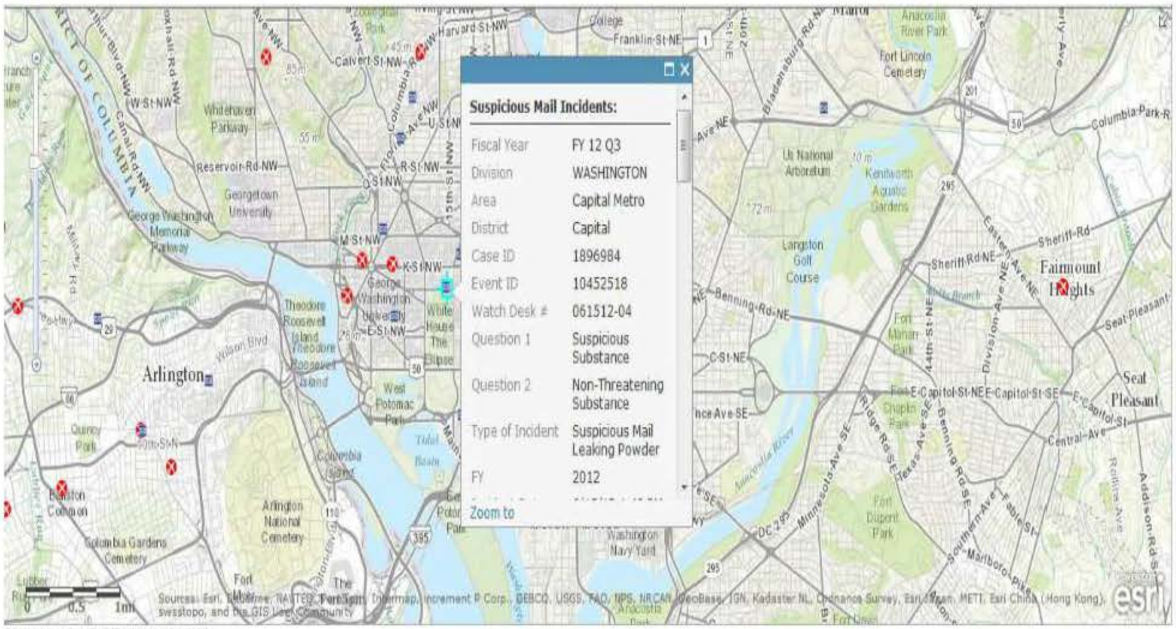
Vancouver
Montreal
Toronto
Detroit
Boston
Philadelphia
Francisco
Gulf of Mexico
MEXICO
Havana
BAHAMAS
0
300
600mi
Sources: Esri, DeLorme, NAVTEQ, TomTom, Intermap, increment P Corp., GEBCO, USGS, FAO, NPS, NRCAN, GeoBase, IGN, Kad
Survey, Esri Japan, METI, Esri China (Hong Kong), swisstopo, and the GIS User Community | Copyright: © 2010 ESRI, AGS

Source: OIG analysis.

[21] We will coordinate the creation of other GIS maps that could be useful to management in enhancing security.

[22] The color coding includes both an outline and fill view by district that can be viewed separately or together or be hidden.

Figure 11: Washington, D.C. Suspicious Mail Incidents and Anonymous Mail (b)(3):39 USC 410 (c) Results



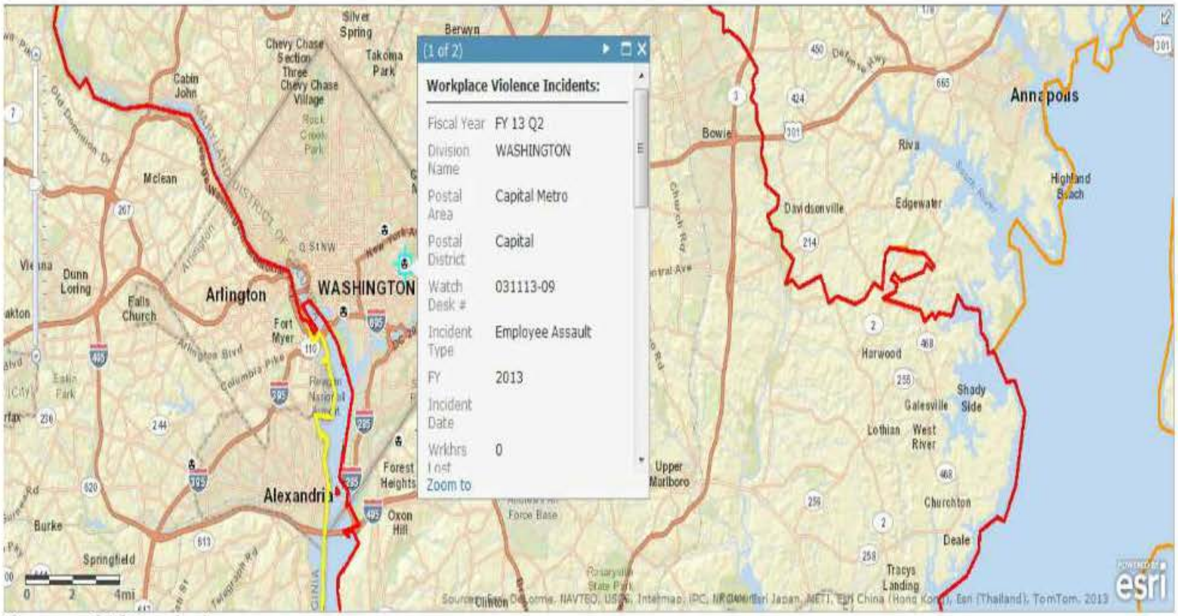
Suspicious Mail Incidents:

Fiscal Year FY 12 Q3
Division WASHINGTON
Area Capital Metro
District Capital
Case ID 1896984
Event ID 10452518
Watch Desk # 061512-04
Question 1 Suspicious Substance
Question 2 Non-Threatening Substance
Type of Incident Suspicious Mail Leaking Powder
FY 2012

Zoom to

Source: OIG analysis.

Figure 12: Washington, D.C. Workplace Violence Incidents and District VOE Results



(1 of 2)

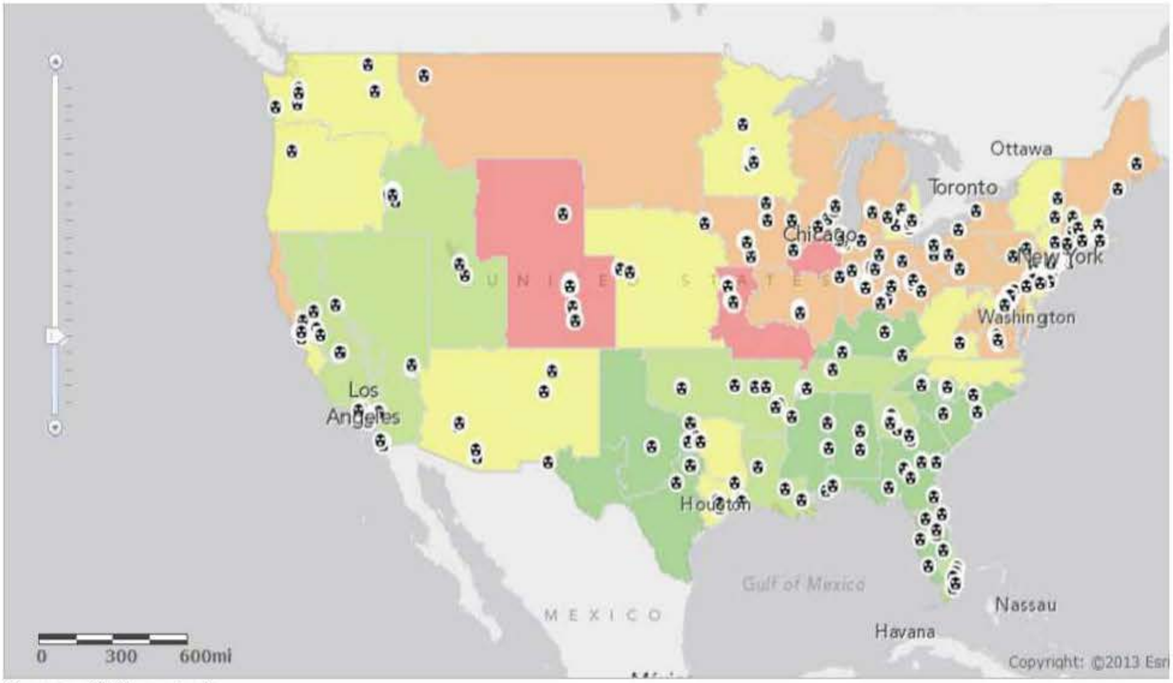
Workplace Violence Incidents:

Fiscal Year FY 13 Q2
Division Name WASHINGTON
Postal Area Capital Metro
Postal District Capital
Watch Desk # 031113-09
Incident Type Employee Assault
FY 2013
Incident Date
Wrkhrs Lost 0

Zoom to

Source: OIG analysis.

Figure 13: Workplace Violence Incidents and VOE Results



Source: OIG analysis.

Figure 14: Washington, D.C. Area Anonymous Mail (b)(3):39 USC 410 (c)(2),(b)(Results and District VOE Results

(b)(3):39 USC 410 (c)(2)

Source: OIG analysis.

Recommendations

We recommend the chief postal inspector:

1. Issue supplemental guidance clarifying roles and responsibilities for homeland security coordinators in assisting districts with anonymous mail follow-up testing and training.

We recommend the Capital District manager, in coordination with the chief postal inspector:

2. Require responsible personnel to take anonymous mail training, including periodic refresher training, and incorporate simulations of the anonymous mail process.
3. Establish controls to ensure responsible personnel are held accountable for complying with anonymous mail requirements.
4. Implement anonymous mail program best practices used by the Nevada-Sierra District, including taking corrective actions for failed facilities.

We recommend the Capital District manager:

5. Establish controls to ensure threat assessment team personnel complete the required workplace violence training, including periodic refresher training, to better understand their roles and responsibilities.
6. Establish controls to ensure responsible personnel complete the workplace violence self-audit tool annually, as required.
7. Establish controls to ensure the threat assessment team adheres to workplace violence policies and procedures.

Management's Comments

Management agreed with all of the findings and recommendations in the report and stated they would take corrective actions to address the recommendations (see Appendix E for management's comments, in their entirety).

Postal Inspection Service management stated that the risk indicators we used in Figure 1 of the report seem to combine elements that are difficult to group together and that it may be more logical to look at the elements individually to generate a composite score and identify at-risk districts. They also stated the suspicious mail analysis seemed to provide little value because it is unlikely to drive change. They further stated that a better indicator would be unwarranted evacuations of facilities stemming from suspicious mail incidents.

Regarding recommendation 1, Postal Inspection Service management stated they are currently conducting a Lean Six Sigma project with the anonymous mail program. Upon completion, they will issue supplemental guidance clarifying roles and responsibilities for homeland security coordinators in assisting districts with anonymous mail program compliance by October 2014.

For recommendation 2, Postal Service district management stated they will require responsible personnel to take anonymous mail training, including periodic refresher training by February 2014. In addition, Postal Inspection Service management stated they will immediately support the Capital District manager with anonymous mail training.

To address recommendation 3, Postal Service district management stated they will establish a quarterly calendar of events for the anonymous mail program to include training, (b)(3):39 USC 410 (c) and compliance reporting by January 2014. In addition, Postal Inspection Service management stated they would establish proper controls to support the Capital District by October 2014, using the findings from the anonymous mail program Lean Six Sigma project.

For recommendation 4, Postal Service district management stated they will implement anonymous mail program best practices used by the Nevada-Sierra District, including service talks to the field, self-audits, and (b)(3):39 USC 410 (c) by January 2014 as well as the use of anonymous mail awareness stickers by March 2014. Further, Postal Inspection Service management stated the findings from the anonymous mail program Lean Six Sigma project will be used to implement anonymous mail program best practices, including those practices utilized by the Nevada-Sierra District by October 2014.

For recommendations 5 and 6, Postal Service district management stated they will require responsible personnel to take workplace violence training, including periodic refresher training by January 2014; and complete the annual workplace violence self-audit tool by September 2014.

Lastly, regarding recommendation 7, Postal Service district management stated the TAT will meet as warranted when situations arise to discuss cases, determine risk factors, and conduct possible follow-up. In addition, management began taking corrective actions stating the TAT will meet by January 16, 2014.

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendations 1 through 6 and partially responsive to recommendation 7. Corrective actions planned for recommendations 1 through 6 should resolve the issues identified in the report. However, with regard to recommendation 7, a major component of the Postal Service's workplace violence prevention program is the TAT. Although district management indicated the TAT will meet as warranted, their response does not establish sufficient controls, including oversight, to ensure the TAT is fully complying with policies and procedures.

Regarding management's concerns about the risk indicators used in Figure 1 of the report, we analyzed each element individually before calculating the average rank and identifying high-risk districts that warrant further review. In addition, the suspicious mail analysis is meant to provide overall awareness regarding the Postal Inspection Service's Dangerous Mail Investigations program. We acknowledge it is difficult to conclude the risks associated with the suspicious mail ranking, but management can use this information to identify anomalies, analyze trends, and follow up on individual incidents to obtain more information on handling and response. Further, as this security risk model evolves, we will continue to coordinate with the Postal Inspection Service to enhance the usefulness of the information and include additional data and analysis as appropriate.

The OIG considers all recommendations significant, and therefore requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. These recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendix A: Additional Information

Background

The Postal Service's security program is designed to maintain integrity and reduce the incidence of crime against people, mail, and other assets. The viability of the Postal Service and its value to the American people depends on having an open and accessible system. A single incident could adversely impact the entire nation, so threats must be taken very seriously. The Postal Service faces a variety of security challenges that require aggressive investigative and preventive responses. Its ability to protect people, the mail, and other assets is fundamental to ensuring high-quality, reliable service.

The Postal Inspection Service's mission is to support and protect the Postal Service and its employees, infrastructure, and customers; enforce the laws that defend the nation's mail system from illegal or dangerous use; and ensure public trust in the mail. To fulfill security and enforcement functions mandated by Congress, the Postal Inspection Service relies on a diverse set of dedicated employees, including postal inspectors; postal police officers; and professional, technical, and administrative specialists.

Objective, Scope, and Methodology

Our objective was to determine whether the Capital District had an effective anonymous mail program to prevent anonymous and potentially dangerous mail from entering the mailstream and a workplace violence program in place to mitigate the potential for violence.

The scope of this review covers the Capital District, which was the (b)(3):39 USC 410 (c)(2) district based on our analysis. Specifically, we obtained, analyzed, and reviewed data related to anonymous mail (b)(3):39 USC 410 (c) results; workplace violence incidents; and suspicious and potentially dangerous mail incidents covering Q3, FY 2012 to Q2, FY 2013. We also incorporated VOE personal safety and security survey responses. As part of our review, we:

- Interviewed Postal Service and Postal Inspection Service personnel responsible for safety and security.

- Assessed current policies and procedures related to anonymous mail, workplace violence, suspicious mail, and VOE surveys.

- Conducted research to identify potential internal and external data for use in our analysis.

- Analyzed anonymous mail (b)(3):39 failures, workplace violence incidents, suspicious mail incidents, and VOE results, and ranked each district.

- Obtained and formatted internal and external security, crime, geographical, and other data to develop GIS maps.

As this security risk model evolves, we will continue to coordinate with the Postal Inspection Service and include additional data or analysis as appropriate.

We conducted this review from June 2013 through January 2014 in accordance with the Council of the Inspectors General on Integrity and Efficiency, *Quality Standards for Inspection and Evaluation*. We discussed our observations and conclusions with management on December 17, 2013, and included their comments where appropriate.

We assessed the reliability of anonymous mail seeding data by reviewing existing information about the data and the methodology used to conduct the seeding, discussing the data with knowledgeable personnel, and conducting limited testing of the data. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

On September 12, 2012, we issued a report on the Postal Service's state of security (*State of Security*, Report Number HR-AR-12-005) and found it has made progress in enhancing security; however, additional opportunities exist to improve security controls and processes. Specifically, the anonymous mail program continues to be ineffective in detecting and preventing potentially dangerous mail from entering the mailstream. We determined the program has been ineffective because carriers do not fully understand their responsibility to identify anonymous mail, and management has not established procedures for identifying facilities that consistently fail to detect it. We also identified insufficient performance measures and training as common problems. As a result, there is increased risk to personnel, the public, assets, and the Postal Service's brand. We made five recommendations to revise and establish anonymous mail procedures, enhance the nationwide anonymous mail seeding program, require additional training, conduct follow-up testing, and establish procedures for identifying and prioritizing security deficiencies. Management agreed with all of the recommendations and has implemented corrective actions to address them.

Appendix B: Anonymous Mail District Rankings and Average Failure Rates

District	Anonymous Mail District Ranking	Anonymous Mail Average Failure Rate
(b)(3):39 USC 410 (c)(2) [redacted]		

District	Anonymous Mail District Ranking	Anonymous Mail Average Failure Rate
(b)(3):39 USC 410 (c)(2) [redacted]		

Source: OIG analysis.

Appendix C: Capital District Facilities Reviewed

Facility
(b)(3):39 USC 410 (c)(2) Processing and Distribution Center
(b)(3):39 USC 410 (c)(2) Post Office
(b)(3):39 USC 410 (c)(2) Post Office
(b)(3):39 USC 410 (c)(2) Post Office
(b)(3):39 USC 410 (c)(2) Post Office Carrier Annex

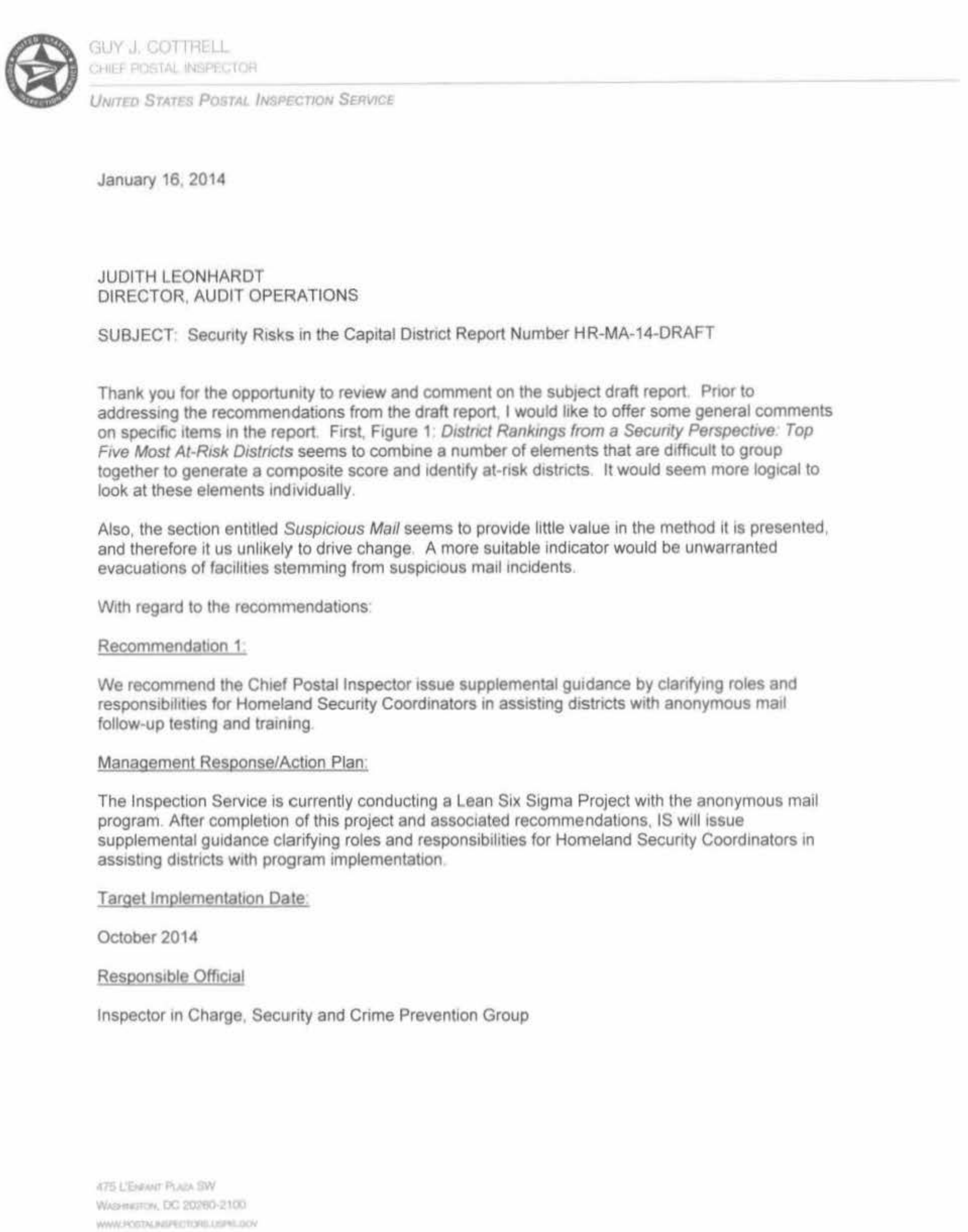
Source: OIG analysis.

Appendix D: Washington, D.C. Crime Statistics

Crime Type	Number of Crimes		Percentage Change
	April 1, 2011, to March 31, 2012	April 1, 2012, to March 31, 2013	
Homicide	103	88	▼15
Sex Abuse	185	265	▲43
Robbery - Excluding Gun	2,945	2,746	▼ 7
Robbery - Including Gun	1,397	1,438	▲ 3
Assault with a Dangerous Weapon - Excluding Gun	1,708	1,712	— No Change
Assault with a Dangerous Weapon - Including Gun	516	555	▲ 8
Total Violent Crime	**6,854**	**6,804**	▼ 1
Burglary	3,711	3,642	▼ 2
Theft	11,374	12,308	▲ 8
Theft of Items from Auto	9,584	9,416	▼ 2
Stolen Auto	3,258	2,842	▼13
Arson	40	39	▼ 2
Total Property Crime	**27,967**	**28,247**	▲ 1
Total Crime	**34,821**	**35,051**	▲ **1**

Source: Washington, D.C. Metropolitan Police Department.

Appendix E: Management's Comments



GUY J. COTTRELL
CHIEF POSTAL INSPECTOR

UNITED STATES POSTAL INSPECTION SERVICE

January 16, 2014

JUDITH LEONHARDT
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Security Risks in the Capital District Report Number HR-MA-14-DRAFT

Thank you for the opportunity to review and comment on the subject draft report. Prior to addressing the recommendations from the draft report, I would like to offer some general comments on specific items in the report. First, Figure 1: *District Rankings from a Security Perspective: Top Five Most At-Risk Districts* seems to combine a number of elements that are difficult to group together to generate a composite score and identify at-risk districts. It would seem more logical to look at these elements individually.

Also, the section entitled *Suspicious Mail* seems to provide little value in the method it is presented, and therefore it us unlikely to drive change. A more suitable indicator would be unwarranted evacuations of facilities stemming from suspicious mail incidents.

With regard to the recommendations:

Recommendation 1:

We recommend the Chief Postal Inspector issue supplemental guidance by clarifying roles and responsibilities for Homeland Security Coordinators in assisting districts with anonymous mail follow-up testing and training.

Management Response/Action Plan:

The Inspection Service is currently conducting a Lean Six Sigma Project with the anonymous mail program. After completion of this project and associated recommendations, IS will issue supplemental guidance clarifying roles and responsibilities for Homeland Security Coordinators in assisting districts with program implementation.

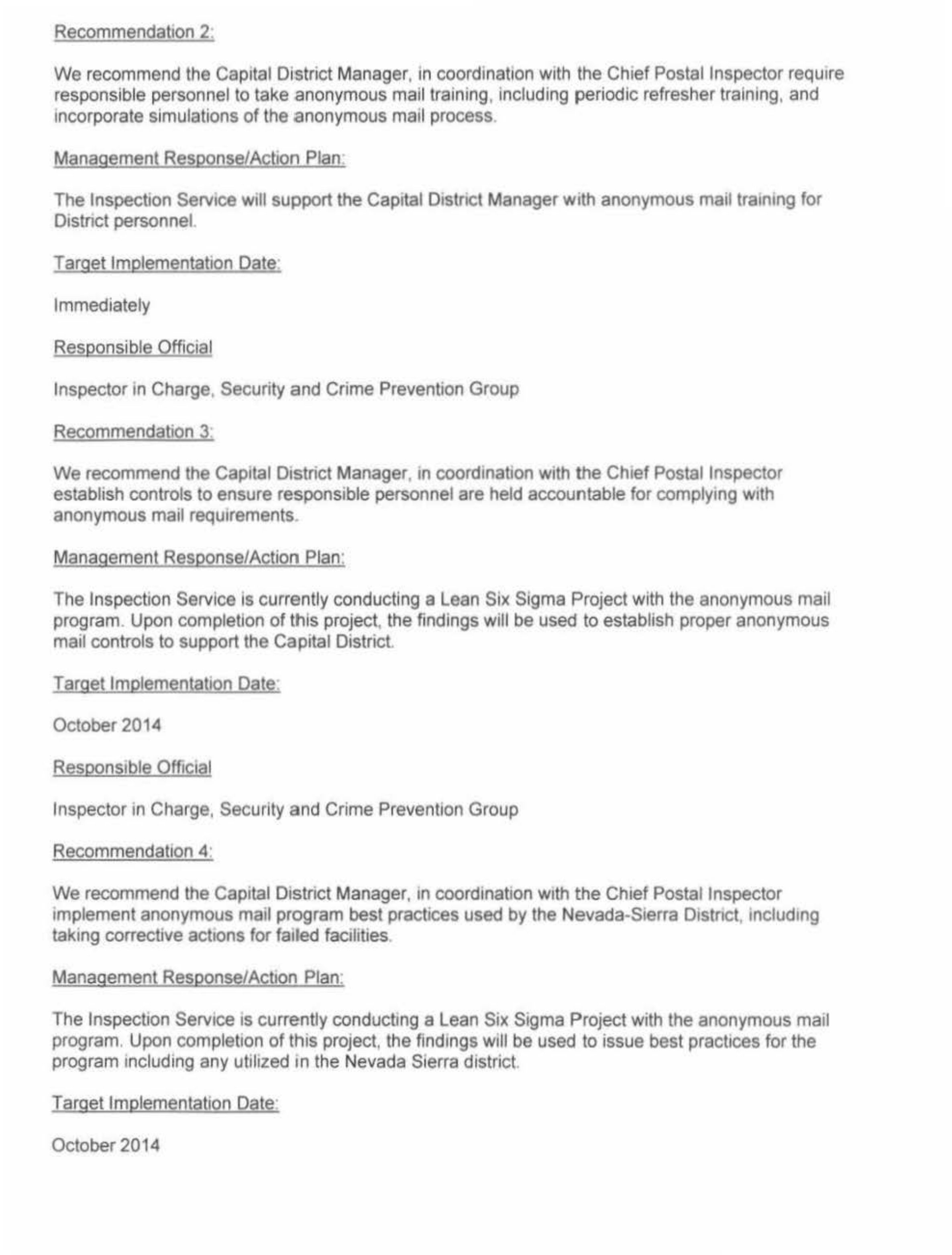
Target Implementation Date:

October 2014

Responsible Official

Inspector in Charge, Security and Crime Prevention Group

475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-2100
WWW.POSTALINSPECTORS.USPIS.GOV



Recommendation 2:

We recommend the Capital District Manager, in coordination with the Chief Postal Inspector require responsible personnel to take anonymous mail training, including periodic refresher training, and incorporate simulations of the anonymous mail process.

Management Response/Action Plan:

The Inspection Service will support the Capital District Manager with anonymous mail training for District personnel.

Target Implementation Date:

Immediately

Responsible Official

Inspector in Charge, Security and Crime Prevention Group

Recommendation 3:

We recommend the Capital District Manager, in coordination with the Chief Postal Inspector establish controls to ensure responsible personnel are held accountable for complying with anonymous mail requirements.

Management Response/Action Plan:

The Inspection Service is currently conducting a Lean Six Sigma Project with the anonymous mail program. Upon completion of this project, the findings will be used to establish proper anonymous mail controls to support the Capital District.

Target Implementation Date:

October 2014

Responsible Official

Inspector in Charge, Security and Crime Prevention Group

Recommendation 4:

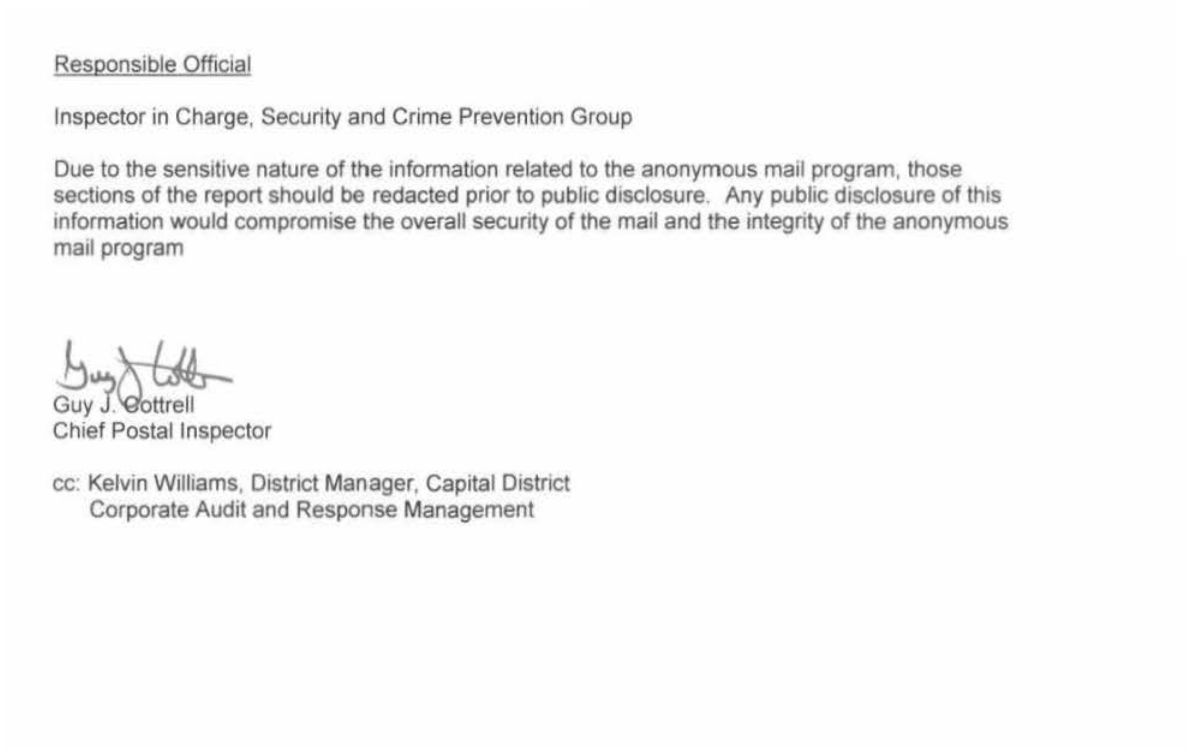
We recommend the Capital District Manager, in coordination with the Chief Postal Inspector implement anonymous mail program best practices used by the Nevada-Sierra District, including taking corrective actions for failed facilities.

Management Response/Action Plan:

The Inspection Service is currently conducting a Lean Six Sigma Project with the anonymous mail program. Upon completion of this project, the findings will be used to issue best practices for the program including any utilized in the Nevada Sierra district.

Target Implementation Date:

October 2014



Responsible Official

Inspector in Charge, Security and Crime Prevention Group

Due to the sensitive nature of the information related to the anonymous mail program, those sections of the report should be redacted prior to public disclosure. Any public disclosure of this information would compromise the overall security of the mail and the integrity of the anonymous mail program

Guy J. Cottrell
Chief Postal Inspector

cc: Kelvin Williams, District Manager, Capital District
Corporate Audit and Response Management

CAPITAL PERFORMANCE CLUSTER
UNITED STATES
POSTAL SERVICE

January 14, 2014

Judith Leonhardt
Director, Audit Operations

SUBJECT: Security Risks in Capital District, HR-MA-14

Thank you for the opportunity to respond to the recommendations the OIG made after completing the audit of Security Risks in Capital District. We have reviewed subject draft and are in agreement with the findings and recommendations as presented.

Recommendation 2:
Require responsible personnel to take anonymous mail training, including periodic refresher training, and incorporate simulations of the anonymous mail process.

Management Response/Action Plan:
Management agrees with this recommendation.

Capital District will work with the Postal Inspector/Homeland Security Coordinator (b)(6) to provide anonymous mail training to the District program coordinators (b)(6) as well as MPOOs, MSCOs and Plant Managers. At the District level, training sessions will be scheduled quarterly for all new supervisors. Periodic refresher training will be provided every 6 months (February and August) for all postmasters, managers and supervisors. We will also ensure Plant personnel are trained and actively involved in the Aviation Security – Anonymous Mail Program. Training methods will include classroom, DVD and WebEx.

Target Implementation Date:
Plant Training – February 2014
District level training - February 2014.

Responsible Official
(b)(6) Manager, Operations Programs Support

Recommendation 3:
Establish controls to ensure responsible personnel are held accountable for complying with anonymous mail requirements.

Management Response/Action Plan:
Management agrees with this recommendation.

The program coordinators (b)(6) will establish a quarterly calendar of events for the Aviation Security – Anonymous Mail Program. The calendar will include training, (b)(3):39 USC 410 (c)(2),(b)(7)(E) compliance reporting. The Manager, Operations Programs Support will ensure the calendar is completed and tasks are timely. The Program Coordinators will monitor compliance, report non-compliance up the chain of command.

Target Implementation Date:
January 2014

Responsible Official:
(b)(6)

Recommendation 4:
Implement anonymous mail program best practices used by the Nevada-Sierra District, including taking corrective actions for failed facilities.

Management Response/Action Plan:
Management agrees with this recommendation.

Capital District will implement the Nevada-Sierra best practices, which will include the FY 2013 Service Talks from the Postal Inspection Service. We will continue monthly self-audit completions. Compliance will be managed through weekly reminders and a monthly report of non-compliance. In addition to management certification that service talks have been given, employees will be randomly queried on the content of the service talk. Training has been addressed in Recommendation 2. Operation Programs Support will (b)(3):39 USC 410 (c)(2),(b)(7)(E) to collection points, including lobby drops, and report out the findings to bring more awareness to the program. We will embrace the anonymous mail awareness stickers in blue collection boxes which Nevada-Sierra District has implemented.

Target Implementation Date:
Service Talks to Field – January 2014
Self-Audits – January 2014
Seeding – January 2014
Anonymous Mail Awareness Stickers – March 2014

Responsible Official:
(b)(6) Manager, Operations Programs Support

Recommendation 5:
Establish controls to ensure threat assessment team personnel complete the required workplace violence training, including periodic refresher training, to better understand their roles and responsibilities.

Management Response/Action Plan:
Management agrees with this recommendation.

Capital District will work with the Postal Inspector/Homeland Security Coordinator (b)(6) to ensure that the Threat Assessment Team personnel complete the required workplace violence training in a timely manner including periodic refresher training to be conducted in Quarter 2 and 4 where the different roles are defined and the team member's responsibilities explained.

Target Implementation Date:
January 2014

Responsible Official:
Manager, Human Resources and the Threat Assessment Team Coordinator.

Recommendation 6:
Establish controls to ensure responsible personnel complete the workplace violence self-audit tool annually, as required.

Management Response/Action Plan:
Management agrees with this recommendation.

The Capital District's LMS Manager will work with the Postal Inspector/Homeland Security Coordinator (b)(6) as well as the Manager of Human Resources to ensure compliance and validation with the annual work place violence self-audit tool.

Target Implementation Date:
September 30, 2014

Responsible Official:
The Manager of Human Resources and the Manager of LMS.

Recommendation 7:
Establish controls to ensure the threat assessment team adheres to workplace violence policies and procedures.

Management Response/Action Plan:
Management agrees with this recommendation.

The Threat Assessment Team meets as warranted when situations arise. The Team will meet to discuss cases, to determine risk factor, and possible follow up. This is also an ongoing process.

Target Implementation Date:
January 16, 2014

Responsible Official:
The Manager of Human Resources and The Threat Assessment Team Coordinator.

Should you need additional information, please contact me. We acknowledge no exemption under FOIA.

Kelvin L. Williams
District Manager