

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault

The image shows a close-up of a heavy, metallic vault door. The door is partially open, revealing a bright blue glow from within. The door has several large, circular mechanical components and bolts. The lighting is dramatic, with the blue glow contrasting against the dark background.

The Black Vault is the largest online Freedom of Information Act (FOIA)
document clearinghouse in the world. The research efforts here are
responsible for the declassification of hundreds of thousands of pages
released by the U.S. Government & Military.

Discover the Truth at: **<http://www.theblackvault.com>**



OFFICE OF THE INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

October 20, 2016

Mr. John Greenewald

via email: john@greenewald.com

RE: FOIA No. 2017-IGFP-00030

Dear Mr. Greenewald:

This responds to your October 18 Freedom of Information Act (FOIA) request to the Office of Inspector General (OIG) for a copy of OIG Management Alert HR-MA-14-002, Mail Isolation, Control, and Tracking, dated December 3, 2013.

I located the document, consisting of 13 pages. I determined the document is appropriate for release with redactions made under FOIA Exemptions (b)(3)^[1], (b)(6)^[2], and (b)(7)(C)^[3], 5 U.S.C. § 552(b)(3), (b)(6), and (b)(7)(C).

If you have any questions regarding the processing of this request you may contact me and/or the FOIA Public Liaison at 703-248-2100. You may also contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is: Office of Government Information Services, National Archives and Records Administration, Room 2510, 8601 Adelphi Road, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

If you are not satisfied with my action on your FOIA request, you may administratively appeal this partial denial. To do so, write to the attention of Gladis Griffith, Deputy General Counsel, 1735 N. Lynn Street, Arlington, VA 22209-2020, within 90 days of the date of this letter. We

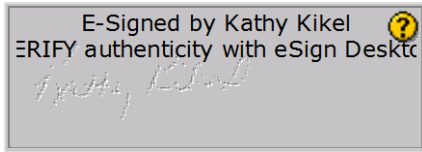
^[1] Exemption (b)(3) provides that agencies may withhold records that are exempted from disclosure by another statute that "establishes particular criteria for withholding or refers to particular types of matters to be withheld." Title 39 U.S.C § 265.6, 410(c)(2) provides that "information of a commercial nature, including trade secrets, whether or not obtained from a person outside the Postal Service, which under good business practice would not be publicly disclosed," is exempt from the disclosure requirements of the FOIA. This exemption was enacted as part of the Postal Reorganization Act of 1970 and operates both independently and as an exempting statute within the scope of Exemption 3.

^[2] Exemption (b)(6) pertains to information the release of which would constitute a clearly unwarranted invasion of the personal privacy of third parties. The withheld material includes names, titles, and identifying information of private citizens. This information is not appropriate for discretionary disclosure.

^[3] Exemption (7)(C) permits the withholding of records or information compiled for law enforcement purposes, the release of which could constitute an unwarranted invasion of the personal privacy of third parties. Lacking an individual's consent or an overriding public interest, third party investigatory records and/or allegations of misconduct must be withheld pursuant to Exemption (7)(C).

accept written appeals via U.S. Mail; e-mail to FOIA@uspsoig.gov; or fax to 703-248-4626. Include the initial request number (e.g., 20XX-IGXX-00XXX) and the date of this letter. Explain what specific action the FOIA Office took that you are appealing. Mark all correspondence "Freedom of Information Act Appeal."

Sincerely,



E-Signed by Kathy Kikel
VERIFY authenticity with eSign Desktop
Kathy Kikel

Kathy Kikel
Government Information Analyst

Attachment



December 3, 2013

MEMORANDUM FOR:

GUY J. COTTRELL
CHIEF POSTAL INSPECTOR

MICHAEL J. AMATO
VICE PRESIDENT, ENGINEERING SYSTEMS

DAVID E. WILLIAMS, JR.
VICE PRESIDENT, NETWORK OPERATIONS

PAT A. MENDONCA
SENIOR DIRECTOR, OFFICE OF THE POSTMASTER
GENERAL

(b)(6)

FROM:

Michael A. Magalski
Deputy Assistant Inspector General
for Support Operations

SUBJECT:

Management Alert – Mail Isolation, Control, and Tracking
(Report Number HR-MA-14-002)

This management alert presents potential human capital, emergency preparedness, and mail security risks associated with the U.S. Postal Service's Mail Isolation, Control, and Tracking processes and mail imaging (Project Number 13YG028DP000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Michael L. Thompson, deputy director, Data Analysis and Performance, or me at 703-248-2100.

Attachment

cc: Corporate Audit and Response Management

Introduction

We initiated our review of the U.S. Postal Service's Mail Isolation, Control, and Tracking (MICT) processes and mail imaging because of media and public privacy concerns related to the ricin¹ events in April and May 2013. In addition, there were public concerns² about the use of mail covers,³ which we will cover in a separate review.

MICT processes were outlined in 2004 as part of the Postal Service's response to a Biohazard Detection System (BDS)⁴ positive alert. BDS was developed in response to the anthrax attacks in 2001. The objective of BDS MICT processes is to identify and recall any potentially contaminated mail and vehicles and to safeguard employees and customers.

The Postal Service uses mail imaging as a tool to enhance the processing and delivery of the mail using automated means. These images are stored on mail processing machines and are used for operational and authorized law enforcement purposes.

Our objective was to assess the Postal Service's roles and responsibilities under MICT.

Background

On April 16, 2013, a First-ClassTM envelope containing a suspicious powder was discovered at the Senate Mail Screening Facility in Maryland. The envelope was addressed to Senator Roger Wicker (Republican-Mississippi) and had no return address. The envelope tested positive for ricin. About 14 Senate employees at the facility were exposed to the envelope and decontaminated. Two additional mailings were subsequently identified, one sent to President Barack Obama and the other sent to Mississippi Judge Sadie Holland.

On May 20, 2013, two letters were mailed and postmarked from the Shreveport, LA Processing and Distribution Center. Each envelope had a typewritten address and contained a threatening note. One letter was addressed to New York City Mayor Michael Bloomberg and the other to The Raben Group.⁵ (b)(7)(C)

(b)(7)(C)

¹ Ricin is a poison found naturally in castor beans. It can be used as a powder, a mist, or a pellet or be dissolved in water or weak acid.

² *The New York Times*, "U.S. Postal Service Logging All Mail for Law Enforcement," July 3, 2013, by Ron Nixon.

³ Mail cover is the process by which a nonconsensual record is made of data appearing on the outside cover of sealed or unsealed class of mail matter. Mail covers are issued only to agencies empowered by statute or regulation to conduct criminal investigations.

⁴ An early warning system used to detect the presence of harmful *B. anthracis* (anthrax) spores that may be released from mailpieces being processed in mail cancellation. Any facility that processes collection mail on an advanced facer/canceller system is equipped with a BDS and ventilation filtration system.

⁵ A Washington, D.C. lobbying, consulting, and public affairs firm.

Postal Service officials stated that the BDS MICT procedures and protocols were not used during the ricin incidents because there was no anthrax and no positive BDS alert occurred.

The Postal Inspection Service used Postal Service operational data from the Advanced Facer Cancellor System 200 (AFCS 200) machine to conduct mail image analysis and worked with the FBI on the ricin investigations. The AFCS 200 is a mail handling system that cancels letter mail, prints an identification tag on the envelope, and generates an image that is used to apply a delivery barcode to mailpieces. The FBI cited the use of AFCS 200 images as part of its investigation of the ricin incidents. This information raised privacy concerns regarding the Postal Service's ability to capture and store images of the mail.

On August 2, 2013, during an Associated Press⁶ interview, the postmaster general (PMG) stated that the Postal Service uses photographs of the exterior of mailpieces primarily for sorting, but makes them available for law enforcement if requested. Images are generally stored for between 7 and 30 days before being disposed. The PMG stated that keeping the images for that period may be necessary to ensure delivery accuracy, forward mail, or make sure proper postage was paid. The PMG also stated that there is no database of the images.

Conclusion

The overall responsibility for the coordination of BDS MICT processes and for mail tracking processes in the event of a suspicious mail incident has not been established. BDS MICT processes are referenced in the Postal Service's *Integrated Emergency Management Plan* (IEMP) template but protocols are incomplete and have not been updated since 2004. As a result, Postal Service employees and customers may be at increased risk of exposure to contamination and the Postal Service's brand could be negatively impacted.

Additionally, we determined the current imaging of mail does not violate a person's rights under the Fourth Amendment, the Privacy Act, or the "sanctity of the seal."

The Fourth Amendment of the U.S. Constitution provides all persons the right to be free from "unreasonable search and seizure." The courts have held that individuals do not have a reasonable expectation of privacy in the information displayed on the outside of an envelope because there is "no reasonable expectation that such information will remain unobserved."

Although it appears that MICT would be subject to the Privacy Act because it requires the Postal Service to collect and maintain images of individuals' mailpieces containing personal information such as names and addresses, the AFCS 200 machines storing these images are not searchable by this personal information. In addition, the "sanctity

⁶ Associated Press, "USPS Takes Photos of all Mail," August 2, 2013, by Andrew Miga.

of the seal” is intended to protect the interior contents of the mail but does not protect information visible on the exterior envelope.

Overall Roles and Responsibilities

Overall responsibility for coordinating BDS MICT and mail tracking processes in the event of a suspicious mail incident has not been established. According to Postal Service officials, MICT is a shared ownership that includes General Counsel, the Postal Inspection Service, Labor Relations, Engineering, and Operations. Another official stated that MICT is mostly executed by the Postal Inspection Service in coordination with Operations, National Preparedness, and Engineering. Management agreed there needs to be clarification regarding ownership of BDS MICT processes. During a meeting, the senior director, Office of the Postmaster General, agreed to take the lead in updating these processes and indicated completion by spring 2014.

Processes for Mail Isolation, Control, and Tracking

BDS MICT processes are incomplete and have not been updated since 2004. Management stated that BDS MICT processes have never been fully implemented because there have been no positive BDS alerts; however, the Postal Service did implement some MICT processes related to upstream mail tracking during the recent ricin incidents. According to the Federal Emergency Management Agency (FEMA), a process for reviewing and revising emergency operation plans (EOP)⁷ should be established. Also, reviews should be a recurring activity and emergency plans should not be in place for more than 2 years without being reviewed and revised. Planning is a continuous process and should evolve as lessons are learned and new information and insights are obtained.

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



⁷ According to FEMA, EOPs are plans that define the scope of preparedness and emergency management activities necessary for that jurisdiction. For example, EOPs assign responsibility to organizations and individuals for executing specific actions that exceed routine responsibility at projected times and places during an emergency.

When a BDS alarm is activated, the installation manager, Emergency Management team (EMT), and the Postal Inspection Service work together to:

- Stop all mail processing.
- Stop the dispatch of all vehicles from the plant.
- Recall vehicles that were dispatched during the test period.
- Redirect vehicles at the facility and those recalled to a quarantine area.

To find the mailpiece that triggered the BDS alarm, personnel are required to identify mail that went through the AFCS 200 within a (b)(3)-39 USC 440 (a)(2) minute window of the alarm. The AFCS 200 identification tags printed on mailpieces are used to identify the specific mailpiece that may have triggered the alarm.

According to the IEMP, Annex 1A, "Biohazard Detection System," district and installation EMT members are responsible for implementing immediate MICT response procedures. EMT members should instruct installations to refuse delivery and redirect trucks with potentially suspect mail back to the affected installation.

As a result of MICT procedures not being fully established, employees, customers, and mail are at risk of harm and the Postal Service's brand could be negatively impacted.

Fourth Amendment, Privacy Concerns, and "Sanctity of the Seal"

We determined that the use of AFCS 200 mail images and images captured by 22 other mail processing systems does not violate a person's rights under the Fourth Amendment. For an act to constitute a "search" under the Fourth Amendment, a person must first have a reasonable expectation of privacy regarding what is being examined.⁸ Courts have held that individuals do not have a reasonable expectation of privacy regarding information that is displayed on the outside of an envelope because there is "no reasonable expectation that such information will remain unobserved."

There are 23 mail processing systems the Postal Service uses that can take images of mailpieces. See [Appendix A](#) for a list of mail processing systems with imaging capabilities, their image retention times, and additional details. We determined the 23 systems are not significant with regard to search and image tracking, although images are retained for various times.

In addition, image records taken from the AFCS 200 and the other 22 mail processing systems are not subject to the Privacy Act. Although mailpieces contain personally identifiable information (PII), such as names and addresses, the machines storing these images are not searchable by PII.

⁸ *U.S. v. Choate*, 576 F.2d 165, 175 (9th Cir. 1978). See also *U.S. v. Huie*, 593 F.2d 14, 15 (5th Cir. 1979). "There is no reasonable expectation of privacy in information placed on the exterior of mailed items and open to view and specifically intended to be viewed by others."

Finally, the imaging of mail does not violate the "sanctity of the seal." The "sanctity of the seal" requirement for most classes of mail is intended to protect the interior contents of the mail but does not protect information visible on the exterior envelope. Unless there is an allegation that the AFCS 200 is breaking the seal on the mailpieces it scans, there is no violation of the "sanctity of the seal" requirement.

Recommendations

We recommend the senior director, Office of the Postmaster General, in coordination with the chief postal inspector and the vice president, Network Operations, and the vice president, Engineering Systems:

1. Designate overall responsibility for the coordination of mail isolation, control, and tracking procedures throughout the Postal Service.
2. Revise and implement formal procedures for mail isolation, control, and tracking to include specific procedures and controls for using mail image information.
3. Ensure that mail isolation, control, and tracking procedures are formally reviewed and updated annually based on lessons learned, new developments, and insights.

Management's Comments

Management agreed with all three findings and recommendations. Regarding recommendation 1, management stated they would designate responsibility for coordinating BDS related-mail isolation and control procedures and updating existing BDS management instructions. Regarding recommendation 2, management stated they will revise and issue formal procedures in their BDS preparedness and response guide. Regarding recommendation 3, management will review and update their mail isolation control and tracking procedures based on lessons learned, new developments, and insights. Management stated they would implement these actions by April 30, 2014. See [Appendix B](#) for management's comments, in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations and corrective actions should resolve the issues identified in the report. The OIG considers all recommendations significant, and therefore, requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective action is 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: Mail Processing Systems with Imaging Capabilities

	Mail Processing System	Image Retention Time	Access Control	Search Capability
1.	AFCS 200	(b)(3);39 USC 410 (c)(2)		
2	Postal Automated Redirection System (PARS) Image Control Tool			
3	PARS subsystem Remote Performance Diagnostic Server			
4	Change of Address Reporting System (COARS)			
5	Image Management System (IMS) PARS			

⁹ General password is a tiered system in which access is granted based on level, operator, supervision, maintenance, national service technician, and Engineering.

	Mail Processing System	Image Retention Time	Access Control	Search Capability
6	COA Scanning	(b)(3);39 USC 410 (c)(2)		
7	Remote Bar Coding System Image Processing Sub System			
8	Remote Computer Reader			
9	Delivery Barcode Sorter, Delivery Bar Code Sorter Input/Output Sub System (DIOSS), and Combined Input/Output Sub System (CLOSS)			
10	AFCS Software Storage Transfer Processor			
11	AFCS-Business Reply Mail Business Image Server			

¹⁰ Imprinted designation and markings on mail that denote postage payment.

	Mail Processing System	Image Retention Time	Access Control	Search Capability
12	Low Cost Reject Encoding Machine	(b)(3); 39 USC 410 (c)(2)		
13	Envelope Reflectance Meter (ERM-III)			
14	Flats Remote Encoding System			
15	Automated Flat Sorting Machine (AFSM-100)			
16	Flats Sequencing System			
17	Automated Parcel/Bundle Sorter			

	Mail Processing System	Image Retention Time	Access Control	Search Capability
18	Automated Package Processing System (APPS)	(b)(3);39 USC 410 (c)(2)		
19	APPS Monitor Display			
20	Web-enabled Automated Package Processing System ¹¹			
21	Passive Adaptive Scanning System			

¹¹ WEBAPAT is an acronym for the Web-enabled Automated Package Processing System (APPS) Processing Results Log Message Analysis Tool.

	Mail Processing System	Image Retention Time	Access Control	Search Capability
22	National Customer Support Center IMS	(b)(3);39 USC 410 (c)(2)		
23	Read Mail Image Notification			

Source: U.S. Postal Service.

Appendix B: Management's Comments

November 22, 2013

JUDITH LEONHARDT
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Management Alert – Mail Isolation Control and Tracking
(Report Number HR-MA-14-DRAFT)

Thank you for the opportunity to respond to the Inspector General's management alert presenting potential human capital, emergency preparedness, and mail security risks associated with the U.S. Postal Service's Mail Isolation, Control, and Tracking processes and mail imaging (Project Number 13YG028DP000).

The Senior Director, in consultation with the Chief Postal Inspector, the vice president, Network Operations, and the vice president, Engineering Systems, agrees with the general findings of this management alert.

Recommendation 1: Designate overall responsibility for the coordination of mail isolation, control, and tracking procedures throughout the Postal Service.

Management Response/Action Plan: Management agrees with this recommendation. The Senior Director's office, in response to this management alert and recommendations made after a HQ BDS exercise was conducted (b)(3):39 USC 410 (c)(2)

(b) will designate responsibility for the coordination of BDS-related mail isolation, control, and tracking procedures in an update to the existing BDS Management Instruction. Responsibility for the coordination of mail tracking processes in the event of a serious suspicious mail incident, such as this past year's ricin mailings, will rest primarily with the USPS, assisted by the Senior Director's office, Network Operations, and Engineering Systems; these coordination responsibilities will be established in a cross-functional protocol that will address policy and procedure for the four functional groups cited.

Target Implementation Date: April 2014

Responsible Officials: Senior Director, Office of the PMG; Chief Postal Inspector

Recommendation 2: Revise and implement formal procedures for mail isolation, control, and tracking.

Management Response/Action Plan: Management agrees with this recommendation. The Senior Director's office, in response to this management alert and recommendations made after a HQ BDS exercise was conducted (b)(3):39 USC 410 (c)(2)

(b) will revise and then deploy formal procedures for BDS-related mail isolation, control, and tracking procedures in the BDS Preparedness and Response Guide, an update to the existing BDS SOP which will obviate the BDS MICT Bridging Document.

Formal procedures for mail tracking processes in the event of a serious suspicious mail incident are being devised through a collaborative process between the four functional groups, and will be established in the protocol cited above. Those component tracking procedures that use mail images captured by processing equipment will be defined and controlled separately by the USPS.

Target Implementation Date: April 2014

Responsible Officials: Senior Director, Office of the PMG; Chief Postal Inspector

Recommendation 3: Ensure that mail isolation, control, and tracking procedures are formally reviewed and updated annually based on lessons learned, new developments, and insights.

Management Response/Action Plan: Management agrees with this recommendation, with a slight amendment. BDS-related mail isolation, control, and tracking procedures, as well as mail tracking processes in the event of a serious suspicious mail incident, will be formally reviewed annually and updated as needed based on lessons learned, new developments, and insights. This commitment to formal review will be made in the BDS MI and in the protocol for serious suspicious mail incidents.

Target Implementation Date: April 2014

Responsible Officials: Senior Director, Office of the PMG; Chief Postal Inspector

Management requests that the OIG consider a complete FOIA exemption for this management alert and management response, due to both law enforcement continuing investigation of the ricin incidents and operational concerns with the disclosure of proprietary mail processing system details captured in both the body and Appendix A of the management alert.

(b)(6)



PAT A. MENDONCA
SENIOR DIRECTOR, OFFICE OF THE POSTMASTER GENERAL

CC: GUY J. COTTRELL
CHIEF POSTAL INSPECTOR

MICHAEL J. AMATO
VICE PRESIDENT, ENGINEERING SYSTEMS

DAVID E. WILLIAMS, JR.
VICE PRESIDENT, NETWORK OPERATIONS