GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

December 20, 2001

The Honorable Dan Burton
Chairman
The Honorable Henry A. Waxman
Ranking Minority Member
Committee on Government Reform
House of Representatives

Subject: Highlights of GAO's Conference on Options to Enhance Mail Security and Postal Operations

As you know, the U.S. Postal Service faces a number of formidable challenges as it seeks to carry out its mission of providing affordable, universal service that binds the nation together. With the recent anthrax attacks on Congress and the media, the Service now faces a new and more immediate challenge of responding to those attacks and developing a plan to safeguard the mail system from future attacks. To assist the Service and its congressional oversight committees in addressing these anthrax-related challenges, you asked that we convene a conference to identify options, other than irradiation, to enhance mail security and postal operations.

On December 10, 2001, we held a conference of representatives from Congress, the Service, and many of the Service's key stakeholders (e.g., major mailers, mailer associations, postal equipment manufacturers, postal unions, management associations, and various federal agencies) to discuss possible options to enhance mail security and postal operations. As agreed, we are providing this letter and its enclosures to document the options identified and the issues that participants raised at the conference for consideration by Congress, the Service, and other stakeholders as they develop strategies to deal with potential terrorist threats to the mail system and enhance postal operations. Enclosure I highlights the options offered by the conference participants, and enclosure II identifies the issues raised as the options were discussed. Enclosure III identifies the conference participants. The options and issues presented here are those of the conference participants and do not necessarily represent our views.

In general, the conference participants agreed that there is no single or simple solution for ensuring the safety of the mail. Nevertheless, they agreed that the Service, the mailing industry, and other stakeholders should work closely together to assess current risks, develop a framework for responding to potential threats, and take immediate steps to secure the safety of the mail to restore public confidence in the integrity of the postal system. Many participants also agreed that detection

technology is essential for securing the mail. They also emphasized the need to enhance the efficiency of postal operations.

Some of the options suggested to enhance mail security and operations included (1) conducting risk-based assessments of potential threats; (2) redesigning and reducing the number of collection boxes to enhance employee and public safety; (3) encouraging the mailing industry to take steps to enhance mail security, such as controlling access to their facilities and participating in a security certification process for bulk mailers; (4) reducing the anonymity of mailers through such measures as requiring identification from mailers and using video-enabled kiosks; (5) creating separate mail streams corresponding to the level of risk associated with the source of the mail; (6) accelerating the Service's implementation of an "information platform" to, among other things, track and trace mail using enhanced bar codes and trackable postage; (7) changing postage rate structures to establish incentives for mailers to promote security, such as discounts and surcharges; (8) communicating a clear and consistent message to employees and the public on security-related matters; and (9) reexamining the postal infrastructure and delivery standards to improve efficiency and security.

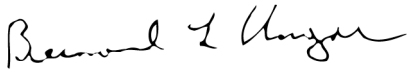
Operational issues raised included the following questions: (1) What risks need to be addressed, such as biological, chemical, radiological, and/or explosive threats? (2) What role should the Service, the mailing industry, and others play in protecting the mail? (3) What impact will efforts to reduce the anonymity of mail have on mailers' convenience and privacy, mail volume, and mail cost? (4) What is the availability of effective detection equipment? (5) What changes can be made to the postal infrastructure to promote both efficiency and security? (6) What security measures need to be taken immediately? and (7) What tradeoffs between mail security and safety, service, convenience, and cost are the public and the mailing industry willing to accept for the nation's mail system?

Public policy issues included (1) whether self-regulation and/or federal regulation is needed to provide oversight of the actions taken by the mailing industry to ensure mail security and how such regulation would be carried out; (2) whether third-party certification of detection and sanitization equipment is needed and who would provide it; (3) whether the Service or another federal entity should be responsible for sanitization of the mail; (4) whether manufacturer liability is hindering the development of detection and sanitization equipment; (5) whether universal postal service should continue to include "anonymous" mail and, if so, on what terms; and (6) who should pay for enhanced mail security—taxpayers, current postal ratepayers, future postal ratepayers, or a combination of these.

- - - - -

We are sending copies of this letter and its enclosures to the Chairmen and Ranking Minority Members of the Senate and House Committees on the Budget; the Chairmen and Ranking Minority Members of the Senate Committee on Appropriations and its Subcommittee on Treasury and General Government; the Chairmen and Ranking Minority Members of the House Committee on Appropriations and its Subcommittee on Treasury, Postal Service, and General Government; the Chairmen and Ranking Minority Members of the Senate Governmental Affairs Committee and its Subcommittee on International Security, Proliferation and Federal Services; the Postmaster General and Chief Executive Officer, U.S. Postal Service; and other conference participants. Copies will also be made available to others upon request.

If you have any questions about this letter or the enclosures, please contact me on (202) 512-8387 or at ungarb@gao.gov.



Bernard L. Ungar
Director, Physical Infrastructure
Issues

Enclosures - 3

Enclosure I

Options Offered by Panel Members and Other Conference Participants for Enhancing Mail Security and Postal Operations

Prevention Options

- Conduct risk-based assessments of potential threats.
- Assess what it takes to create the threat and to deliver, detect, and counter it.
- Ensure that countermeasures address the problem instead of deterring something that might not be repeated.
- Educate employees on safe mail handling and the proper use of protective gear.
- Educate secondary and tertiary vendors regarding the need for heightened security.
- Ensure that incident response plans are in place for facilities that receive and process high volumes of inbound mail.
- Require that mailpieces have bio liners that can kill bacteria.
- Develop and implement a security certification process for bulk mailers.
- Distribute posters alerting mail preparation personnel and the public of the penalties for hoaxes in the mail, and prosecute perpetrators to the fullest extent of the law.
- Ensure that professional mailers have adequate procedures in place to
  - strictly control access to their plants and work sites, such as requiring deliveries to be made to restricted areas;
  - secure transportation by taking such steps as sealing all inbound and outbound shipments, using certified trucking companies; and recording and checking the serial numbers of the seals on bills of lading;
  - provide for a secure workforce by performing background checks and establishing an employee identification program; and
  - provide for adequate mailpiece design by such actions as using transparent, tamper-resistant envelopes; a recognizable company logo on the outside of mailpieces; and indicia or metered postage instead of live postage stamps.
- Develop standards for safe and secure bulk mail.
- Employ a mailer certification process.
- Independently assess the security operations of bulk mailers.
- Deny bulk mailers' access to the mail system if they do not provide secure mail.

Options to Reduce the Volume of Anonymous Mail

- Issue "smart cards" encoded with "official" postal identification information (i.e., identity, postal address, and e-mail address).
- Allow the use of postal smart cards at video-enabled kiosks located in various retail sites.
- Require presentation of a driver's license and/or credit card or debit card when purchasing stamps or mailing packages. An alternative would be to allow smart cards to provide identification.

- Expand retail presence in kiosks and mail service centers in food retail stores to make services involving identification available.
- Develop envelopes with windows for both the mailing address and return address that could be used for remittance mail.

Detection Options

- Equip collection boxes and mail slots with plastic bag liners that have one-way throats and detection strips for a wide variety of bacteria.
- Provide postal workers with contamination detectors, which would be worn on their breast pockets like radiation badges.
- Equip postal facers/cancellers with scanners that will alarm if they come in contact with a threshold level of a contaminant.
- Use portable sampling devices to detect contaminants on the surface of packages or in mail sacks and trays.
- Deploy currently available detection and sanitization technology—do not delay deployment while waiting for more advanced technology to be developed.
- Develop detection strips for mailboxes and require that these strips be installed in all mailboxes, including rural mailboxes and cluster boxes.
- Use third parties to certify the capabilities of detection and sanitization technologies before procuring and deploying.

Mail Collection Options

- Conduct a comprehensive review of all collection boxes and mail slots and determine if some of them could be eliminated because they are either served by a local post office or infrequently used.
- Use sampling teams to test detection systems, such as those employed on collection boxes with detection strips.
- Consider requiring cluster boxes for some existing housing.

Mail Preparation Options

- Use current technology to sanitize mail.
- Use available filtration systems to screen mail contaminants.
- Require that windowed envelopes be closed with a protective film to help prevent cross contamination.
- Require that bulk mailers use tinted shrinkwrap for their mail, thus identifying the mail as coming from a professional mailer and allowing for easier detection of tampering.
- Require that film processors use transparent plastic envelopes with “safety” seals.

Enclosure I

Mail Processing Options

- Optimize the postal infrastructure to reduce redundancies.
- Install high-efficiency filtration systems within postal mail-processing facilities to minimize the spread of contaminants from the mail.
- Develop and deploy filtration systems for mail-processing equipment to identify and limit the spread of contaminants from the mail.
- Create three separate mail streams corresponding to the level of risk associated with the source of the mail. That is, high-risk anonymous mail (e.g., mail from collection boxes on the street), medium-risk semi-anonymous mail (e.g., packages and other mail handed to a window clerk), and low-risk mail (e.g., bulk mail from a known shipper).
- Do not merge collection mail with bulk mail until decontamination testing of the collection mail has been completed to help prevent cross contamination.
- Test sanitization equipment on actual anthrax spores. Do more testing of the impact of sanitization on different types of mail.
- Task a federal organization other than the Service with responsibility for operating and financing the sanitization equipment.

Options for Tracking Parcels and Other Mail

- Develop and deploy an information platform that will allow the Service to track and trace mailpieces and provide customers with real-time information on the status of their mailings.
- Digitally watermark and/or have indicia on all stamps and prestamped envelopes to allow them to be tracked and traced by lot number and by the post office that sold them.
- Update the Service's Point-of-Sale (POS) system with a transaction-based database that will provide the capability to record stamp sales by type, lot number, and purchaser's name and address.
- Market PC postage more widely—for example, through kiosks. PC postage products create Information Based Indicia—a two-dimensional (2D) bar code to convey security and mail-processing information about the mailpiece.
- Issue "official" USPS e-mail addresses.
- Develop database cross-linking e-mail and postal addresses to enable businesses to use hard-copy mail when customers do not respond to e-mail.

Options for Using Information Technology to Create "Intelligent Mail"

- Expand the use of two-dimensional bar code technology to provide additional data for tracking the mailpiece and make this technology available to all mailers.
- Redesign the Domestic Mail Classification Schedule (DMCS) to provide mailers with discounts to encourage maximum participation in programs that enhance mail security and the Service's cost efficiency.

Enclosure I

Infrastructure or Network Options

- Reexamine the entire postal system to improve both mail security and safety as well as postal operations.
- Expand the Service's retail presence through the use of kiosks and "mail service" centers located in food retail stores.

Rate Structure or Pricing Options

- Change the postage rate structure to establish incentives for mailers to promote mail security, such as surcharges, discounts, and/or new mail classes or subclasses.
- Divide First-Class Mail into two new subclasses—(1) single-piece mail that requires additional security handling by the Service and (2) bulk mail from presort houses that requires no additional handling.
- Create a new class of mail, such as "Second-Class Mail." This mail would be sealed against inspection and subject to slower delivery than First-Class Mail. Second-Class Mail could include anonymous mail, such as greeting cards, and would be irradiated.
- Establish discounts for PC postage.

Options for Changing Delivery Standards to Enhance Mail Security

- Provide for discounts or different delivery standards for mail based on the level of security standard met.

Options for Financing Costs Relating to Mail Safety and Security

- Increase postage rates.
- Increase limits on the Service's borrowing authority.
- Impose a surcharge on anonymous mail that requires more safety or security measures, such as sanitization.
- Congress could appropriate funds to cover the additional security-related costs since September 11, 2001. (Appropriations to the airline industry would be a good model to follow.)
- Congress could fund any requirements to irradiate mail and to provide special handling and safety measures for government mail.
- Congress could appropriate funds to enable the Service to complete the information platform in a much shorter time frame than would otherwise be the case.
- Require mailers to initiate safety and security measures and bear the cost.

Enclosure I

Options for Responding to Incidents

- Have call centers for employees, customers, and postal operations.
- Communicate a clear and consistent message on the incident and what is being done.

Other Options

- Build public confidence in the integrity of the mail system by communicating steps being taken to provide for a secure and safe mail system.
- Create a greater deterrent by communicating the ability to identify the perpetrators of threats and hoaxes as well as the consequences of these crimes.
- Rely on the mailing industry to communicate the importance of mail and the mailing industry to Congress and the public.
- Review privacy statements on whether the Service will pass along customer information.
- Clearly mark all bulk mail shipments.
- Update or create business continuity plans for critical postal functions.
- Include mailing industry representatives on the Communicating and Messaging Working Group of the Postal Service's Mail Security Task Force.

Enclosure II

Issues Raised by Panel Members and Other Conference Participants Regarding Mail Security and Postal Operations

Issues Raised

- What tradeoffs between mail security and safety, service, convenience, and cost are the public and the mailing industry willing to accept for its mail system?
- To what extent should the mail system be accessible and enable customers to send "anonymous mail?" Should such mail be surcharged?
- Are sufficient financial resources available to implement improvements? What level of cost is appropriate—is there some limit on what is worth doing, considering the risk? What will be the impact of costly measures? Are decisions being overly influenced by the associated cost?
- What risks need to be addressed, including biological, chemical, radiological, and explosive risks?
- What is the objective (e.g., to detect and deter risks or to restore public confidence)? To what extent do different objectives call for different approaches?
- What level of detection or sanitization will be required to maximize public confidence in the safety of the mail?
- To what extent should the Service provide a universal system with measures to help ensure mail security and safety? Should measures taken by the mailing industry be considered sufficient for its mail to bypass some or all of the Service's measures (e.g., drop-shipped mail that could avoid sanitization and/or detection)?
- Should irradiation be the Service's primary method of securing the mail or should it be placing more emphasis on such efforts as early detection of contaminated mail, developing an information platform, tracking and tracing, and smart stamps? Is cost-effective detection technology available that can be fully deployed for all mail, including mail drop-shipped to post offices?
- What is the appropriate balance between the public's right to privacy versus the Service's need to know the identity of mailers in order to increase mail security?
- What can be done to reduce anonymous or unknown mailers?
- How can the Service and the government best assess the risks associated with using the mail system for terrorist purposes and develop an appropriate framework to respond to threats?
- Who should bear the additional cost associated with securing the mailstream—taxpayers, current postal ratepayers (through rate increases), future postal ratepayers (through borrowing), or a combination of these? If current ratepayers are to bear the additional cost, how should that cost be allocated?
- What role should mailers play in protecting the mails? What role should their suppliers play (e.g., envelope suppliers and paper mills)? Should there be a different standard for the Service and others (e.g., in the filtration and detection equipment used)?
- Are there lessons to be learned from foreign postal administrations that could improve postal operations and better protect the mail?

- Should the Service purchase currently available technology to detect contaminants and sanitize the mail, or should it delay those purchases until better technology is available?
- Who should be liable in the event of terrorist acts involving the mail? Should liability be capped? Is third-party product liability hindering efforts to develop and implement new technology to detect contaminants and sanitize the mail?
- Does the Service's current infrastructure promote maximum effectiveness and efficiency?
- How should the Service process mail that is known to be sensitive to current sanitization technology, such as photographic film and pharmaceutical products?
- What legislative changes, if any, might be needed to improve postal operations and protect the mail from terrorists?
- Who decides whether measures taken by mailers are adequate to protect mail security and safety? Is self-regulation adequate to ensure mail safety and security and public confidence, or is federal regulation and oversight needed to ensure that the mailing industry has taken adequate measures?
- If federal regulation is needed, would there be standards against which to regulate? Who would have responsibility for regulation: the Service, the Occupational Safety and Health Administration, the Postal Rate Commission, and/or other federal agencies? What enforcement mechanism is appropriate?
- Should sanitization and detection equipment receive third-party certification? Would this be a federal responsibility? If so, how can this be done with the current limited testing capacity?
- How quickly does progress need to be made? Do different time frames apply to different measures?
- How should the Service be held accountable for making progress on such steps as the information platform?
- Whose job is it to convince the public that the mail is safe: the Service, the mailing industry, or Congress?
- Who is going to follow-up on the options and questions raised at the conference?
- What impact will efforts to reduce the anonymity of mail have on mailers' convenience, mail volume, mail cost, and mailer privacy?

Panelists and Other Participants of the GAO Conference on Options to Enhance Mail Security and Postal Operations

Introductions

The Honorable David M. Walker
Comptroller General of the United States
U.S. General Accounting Office

Bernard L. Ungar
Director, Physical Infrastructure Issues
U.S. General Accounting Office

Jack Potter
Postmaster General, CEO
U.S. Postal Service

The Honorable Henry A. Waxman
Ranking Minority Member, Committee on
Government Reform
House of Representatives

The Honorable Ernest J. Istook
Chairman, Subcommittee on Treasury,
Postal Service, and General Government
Committee on Appropriations
House of Representatives

Panel 1: Options for the Postal Service to Enhance Mail Security and Postal Operations

Mary Elcano - Moderator
Sidley Austin Brown & Wood LLP

Allan Algazi
Symbol Technologies

Maynard Benjamin
Envelope Manufacturers Association

John Campo
Pitney Bowes, Inc.

Richard Fairfax
Occupational Safety and Health Administration

Michael Schmidt
Deutsche Post World Net

Ken Weaver
U.S. Postal Service

Panel 2: Options for Mailers to Enhance Mail Security and Postal Operations—Mail Preparation and Information Technology Strategies

Gene A. Del Polito - Moderator
Association for Postal Commerce

John Campanelli
R.R. Donnelley Logistics Services

Eric Casey
Mailing & Fulfillment Service Association

Judy Marks
Lockheed Martin Distribution Technologies

V. Joseph Renna
Pharmaceutical Care Management Association

Seth Weisberg
Stamps.com

Summary of Conference

David Treworgy
PricewaterhouseCoopers LLP

Other Participants

Alison Bean
Senate Committee on Governmental Affairs

Brooke Brewer
Senate Committee on Governmental Affairs

Peter Dees
Senate Committee on Governmental Affairs

Nanci Langley
Senate Committee on Governmental Affairs

Susan Propper
Senate Committee on Governmental Affairs

Robert Westbrooks
Senate Committee on Governmental Affairs

Tammy Hughes
House Appropriations Committee

Ed Puccerella
House Budget Committee

Kate Anderson
House Committee on Government Reform

Phil Barnett
House Committee on Government Reform

Andrei Greenawalt
House Committee on Government Reform

Michael Layman
House Committee on Government Reform

Denise Wilson
House Committee on Government Reform

Nick Manetto
House of Representatives

William Heniff
Congressional Research Service

Frank Brennan
U.S. Postal Service

Tom Day
U.S. Postal Service

Sheila Meyers
U.S. Postal Service

John Rapp
U.S. Postal Service

Jim Roman
U.S. Postal Service

Wayne Wilkerson
U.S. Postal Service

Dave Willard
U.S. Postal Service

Len Read
Office of the Inspector General
U.S. Postal Service

Robert Cohen
Postal Rate Commission

Daniel LaPlaca
Office of Management and Budget

Dr. Lawrence D. Kerr
Office of Science and Techology Policy

Dr. Jeffrey S. Kieft
Office of Science and Techology Policy

Clint Chamberlain
Office of Public Health Preparedness

Brian Little
Occupational Safety and Health Administration

Dr. Kevin D. Crowley
National Academy of Sciences

Hans Martin
Federal Bureau of Investigation

Melissa Willig
Federal Bureau of Investigation

Henry Maury
General Services Administration

Neil A. Boyer
Department of State

Linda Elliot
D.C. Circuit Court

Enclosure III

Michael Reid
American Postal Workers Union

Al Ferranto
National Association of Letter Carriers

Dick Collins
National Postal Mail Handlers Union

Dale Holton
National Rural Letter Carriers Association

Ted Keating
National Association of Postal Supervisors

Bob Levi
National Association of Postmasters of the United States

Joe Cinadr
National League of Postmasters of the United States

Tony Gallo
Association for Postal Commerce

Peter Jacobsen
Association for Postal Commerce

Robert Laybourn
Association of Priority Mail Users, Inc.

Edward Hudgins
Cato Institute

Ari Schwartz
Center for Democracy & Technology

Edward Gleiman
Direct Marketing Association

Russ Snyder
Greeting Card Association

Robert E. McLean
Mailers Council

Cecilia Daly
Magazine Publishers of America

Enclosure III

David Todd
Mail Order Association of America

Jack Estes
Main Street Coalition

Robert J. Brinkman
Newspaper Association of America

Joel Thomas
National Association of Presort Mailers

Senny Boone
National Newspaper Association

Mike Cavanagh
National Postal Policy Council

James Pierce Myers
Parcel Shippers Association

Brett Martin
Pharmaceutical Care Management Association

Wolfgang Pordzik
Deutsche Post World Net USA, Inc.

David Nassef
Pitney Bowes, Inc.

David Zaharchuk
PricewaterhouseCoopers LLP

Robert Grabowski
Symbol Technologies

(543015)