Office of Governmentwide Policy

GSA Policy Advisory: National Guidelines for Assessing and Managing Biological Threats in Federal Mail Facilities

December 29, 2003

I. Introduction

In October 2001, terrorists contaminated the U.S. mail stream with anthrax, resulting in illness and death of federal employees and the public. The threat of similar attacks continues, and the authorities have been called in to assess numerous hoaxes and suspect materials. To protect the health and safety of federal employees and the public, and to help deal with hoaxes and suspicious materials, federal agencies need clear procedures for assessing and managing biological threats that might be delivered in the mail.

GSA has developed this new set of guidelines as standard operating procedures for dealing with any type of biological threat, in federal mail centers nationwide. These guidelines have been developed in coordination with a distinguished group of federal and non-federal scientists and other experts (the individuals and organizations participating in the group are listed in Appendix A). They replace the previous " Guidelines for Federal Mail Centers in the Washington, DC Metropolitan area for Managing Possible Anthrax Contamination" published July 22, 2002 and "National Guidelines for Assessing and Managing Biological Threats in Federal Mail Facilities" published in July, 2003. As before, GSA is issuing these guidelines as part of its responsibilities to the federal mail management community under the Federal Records Act (44 U.S.C 2904).

The guidelines are arranged in five areas:

- The all – hazards approach
- Preparing for biological threats
- Identifying and assessing biological threats
- Managing biological threats that appear credible
- Sampling, testing, and sanitization.

GSA intends these guidelines for use by:

- Mail center workers in federal facilities nationwide;
- Managers of those facilities;

- Environmental health and safety officers responsible for mail center workers; and
- Federal executives responsible for mail operations.

In the integrated threat assessment and response to any threat, the federal officials listed above must engage with a set of federal and non-federal partners, including:

- Local first responders to federal mail centers (fire, hazmat, and law enforcement);
- Local public health authorities (disease control and laboratory);
- Regional Federal Bureau of Investigation (FBI) Weapons of Mass Destruction (WMD) coordinators;
- Local US Postal Inspectors.

Definition of a "first responder": A "first responder" is an organization in your immediate area that provides trained people to respond to emergency situations. You may need to establish relationships with several different first responder organizations, depending on the personnel and capability that they can provide. First responders to federal mail facilities may be federal, state, and/or local organizations, depending on your specific circumstances.

Definition of a "federal mail center": A federal mail center is a defined space where the mail for a federal agency is processed.

II. The All-Hazards Approach

Many different threats can be sent through the mail. The initial triage, or sorting and allocation of treatment to individuals according to a system of priorities for any threat situation, must consider *all* hazards. A critical element is assessing for the presence of:

- Radiological threats;
- Explosive devices;
- Dangerous chemicals; and
- Biological threats.

Effective, well-tested procedures exist for detection and response to explosive devices, chemicals, and radiological materials. This document is specifically designed to deal with suspected biological threats. This section highlights one important difference in approach between biological threats and other threats. Chemical and radiological agents are rapidly known and require immediate consequence management. Biological agents, on the other hand, are not as immediately recognizable and consequence management may be delayed, for example by therapy or vaccination, not traditionally performed by first

responders. However, effective countermeasures are available against many of the bacteria, viruses, and toxins that might be used. If we develop a solid understanding of the biological threats we face and how to respond to them, many effects may be prevented or minimized. An on-line course on "Biological Agents in the Mail Center" is also available at www.gsa.gov/mailpolicy.

In response to a suspected known or suspected release of a chemical or radiological agent, authorities may recommend that you "shelter in place." This means that, rather than leave the place of work, employees should stay in their office buildings and wait for instructions.

In a chemical attack, a toxic gas or liquid is used to contaminate people or the environment. The prevalent symptoms are tightness in the chest, difficulty breathing, blurred vision, stinging of the eyes, or loss of coordination. If you witness a suspected chemical attack outdoors, move upwind and away from the area as quickly as possible. If this is not possible, move to a safe location inside a building and shelter in-place. If you suffer any of the symptoms mentioned above, try to remove any clothing you can and wash your body with soap and water. Do not scrub the area, as this may wash the chemical into the skin. Seek medical advice as soon as possible.

Dirty bombs are regular explosives that have been combined with either radiation-causing material or chemical weapons. While most news reports talk about radiological dirty bombs, chemical agents may be used as well. A blast from this type of weapon normally looks like a regular explosion, and the contamination spread is not often immediately noticeable. When it is safe to do so, seek shelter inside a building or basement, putting as much shelter between you and the potential contaminant as possible. Limit the amount of exposure by leaving the area when it is safe to do so.

Additional information on dealing with the other types of threats may be obtained from sources listed in Appendix D. This document may be used to help develop a better understanding of the biological threats we face and the steps to take if a biological agent is suspected of being sent through the mail. As the anthrax bio-terrorism events in 2001 illustrated, mail supervisors sometimes need to make judgments about mail that relate to their security in receiving it. This document is intended to provide a more effective process for federal employees to screen their mail.

III. Preparing for biological threats

A biological threat is any biological material capable of causing:

- Death, disease, or other biological malfunction in a human, an animal, a plant, or another living organism;

- Deterioration of food, water, equipment, supplies or material of any kind;
- Harmful alteration of the environment.

Advance preparation is critical to assessing and managing any biological threat that may come in the mail. This section offers short discussions of the key preparation steps. Every mail center should have a written security plan. The plan should include the topics listed below. The U. S. Postal Inspection Service (www.usps.com/postalinspectors) and the GSA mail policy website (www.gsa.gov/mailpolicy) both provide much more detailed guidance on all of the following topics:

Security assessment: Start with a site-specific security assessment, conducted by a qualified expert. Recognize that each site has different threats and risk levels, and that this will lead to different security measures for each site. The *GSA Mail Center Manager's Security Guide* (www.gsa.gov/mailpolicy) includes a list of resources for security assessments.

Relationships with partner organizations:

- Establish and maintain relationships with all of the key partners listed in Section I (i.e., first responders, etc.).
- Determine who will be responsible for opening unopened suspicious letters and packages in your facility, and establish a relationship with them (this may be a specially trained federal personnel or other first responders).
- Establish relationships and protocols with the local Federal Bureau of Investigation (FBI) WMD Coordinator concerning suspicious powders and liquids, or make sure that your first responders have done so.
- Ensure that the first responder organization(s) are ready, willing, and able to follow the established protocols, including these guidelines, and that they have relationships with the other key partners.

Many of the above preparedness activities and local government contacts can be initiated through and coordinated with the Local Emergency Planning Committee (LEPC) responsible for the mail center's geographic location. LEPC contact information can be found at http://www.epa.gov/ceppo/lepclist.htm.

Training and rehearsal: All mail center security procedures should describe how current and new mail center workers will be trained and how they will routinely rehearse various plans and scenarios. Signs should be posted in every mail center that list suspicious characteristics and that clearly identify whom to contact for each of the various types of threats.

X-ray inspection and suspicious characteristics: Before sorting or internal delivery, all mail delivered to federal agencies should be inspected by an x-ray machine operated by trained personnel. Small facilities should consider

partnering with a larger facility to inspect by x-ray. **All deliveries from couriers and express carriers (e.g., FedEx) should be x-rayed as well.** In addition, mail center workers must monitor the mail continuously for suspicious characteristics (See Appendix C for the standard list of suspicious characteristics). As described below, procedures must be in place, with continual training and rehearsal, for dealing with any mail that appears suspicious.

Communications: Security procedures should specifically identify the agency managers and agency public affairs officials who will coordinate all internal and external communications in the event that a threat appears to be credible. Security procedures should also ensure that:

- Internal and external audiences are identified in advance;
- All available information is communicated in a timely manner;
- Everyone is sending the same message;
- All facts are confirmed with competent authorities;
- Designated communicators also have designated backups;
- Local union officials are involved;
- Local public health and local law enforcement officials are included in the communications chain;
- Messages are crafted so that all personnel can easily understand the information; and
- Results of any laboratory tests are communicated as quickly and completely as possible, including detailed, quantified results whenever quantitative tests were used; in any case, you should provide details about the nature of the tests that were used and the limitations, if any, of the test methods and results.

Security procedures should also identify which audiences may be informed of threats before they have been confirmed; e.g., local health officials may want to know that samples have been taken for analysis. They should also include specific information on prompt communication of any available test results, specifying the testing methods used, and explaining the limitations, if any, of both the results and the testing methods.

The Occupational and Health and Safety Administration (OSHA) requires that a Health and Safety Plan (HASP) be developed for any clean-up of hazardous materials (see http://www.osha.gov/dep/anthrax/hasp/).

Additional Considerations in Preparation are listed in Appendix B.

IV. Identifying and assessing biological threats

When working with mail and identifying if a mail piece is suspicious or the FBI needs to be contacted, **two scenarios should be reported to the FBI WMD**

Coordinator. Initially, the designated first responder such as the Federal Protective Service (FPS), Defense Protective Service, or other first responder, would be notified. They would then ensure that the FBI WMD Coordinator is notified in these two scenarios:

Opened mail that is leaking a suspicious liquid or powder, or mail that has a suspicious odor: If you open a letter or package and see an unknown material, or if an unknown material is leaking from the mail as a liquid, powder, or odor, *do not try to clean it up or otherwise disturb it*. Set the mail down on a stable surface and call the first responder designated to respond to this type of threat.

Opened mail that contains a written threat: If anyone in the organization opens a letter or package *with or without powder* and discovers a written threat, such as a note that says "You have been infected with anthrax," put the package or letter down on a stable surface and call the first responder designated to deal with this type of threat. The mail center supervisor or the first responder must ensure that the FBI local WMD Coordinator is notified in either of these events.

A much more common scenario is a letter or package that is unopened and appears suspicious. Consider the following:

Unopened mail: Whenever a mail center worker identifies an unopened package or letter as "suspicious", a mail center supervisor or specially trained employee should examine the mail piece to confirm that it meets the criteria established for the location. If confirmed, *do not open it.* A supervisor or designated mail center worker who is trained to confirm the identification must be available during all working hours.

Next, determine if the mail piece is addressed to a person who actually works in the facility. If so, and if the addressee can be located in a reasonable period of time, contact the addressee and ask him or her to identify the package. If the addressee recognizes the package and is certain it is not threatening, deliver it. If the addressee does not recognize the package, or if you cannot locate the addressee, attempt to contact the individual listed on the return address to verify the contents of the package. If you successfully contact the sender of the package, ask them to provide a description of the contents, intended addressee, and the reason it was mailed to your location. Provide this information to the addressee for further verification.

If the addressee does not recognize the package, or if you cannot locate the addressee, *do not open it.* The supervisor or designated mail center worker should call the previously designated first responder (that is, the organization you have identified as the right one for the specific threat in hand). This first responder will be responsible for opening the package in a

controlled environment and following the appropriate protocol for evaluation of the threat. A "controlled environment" may be a glove box, hood with negative airflow and HEPA filters on the exhaust airflow, or a similar device. When identifying the first responder who will open suspicious letters or packages, make sure they have such a device available.

Mail that contains an unidentified secondary container: If x-ray inspection shows a secondary container that may contain an unknown material, or if you open a letter or package and discover such a container, *do not open or otherwise disturb the secondary container*. Treat the secondary container as suspicious, unopened mail. As above, first call the addressee and see if they can identify the container. If he or she cannot be located, then call in the first responder designated to open suspicious mail.

The USPS is irradiating much of the mail that is being delivered to federal agencies in the Washington DC, metropolitan area. The procedures for identifying and assessing biological threats are the same, as described above, for locations where the USPS is irradiating mail. That is, irradiation does not change the process described in this section.

V. Managing biological threats that appear credible

In the event that a trained first responder, after reviewing the situation, determines that a possible biological threat may actually be present (i.e., a biological agent may have been released into the workplace, or a biological agent may be present in a package or envelope that has been opened as discussed above), the **first responder** should take the following steps or ensure that these activities are performed where appropriate:

- Turn off the ventilation system, fans or window air conditioners for the area of potential release.
- Turn off any high-speed mail processing equipment that may have handled the suspicious mail piece.
- Make sure that the suspicious substance is not disturbed by covering it or bagging it if appropriate.
- Keep everyone out of any room(s) that may have been contaminated.

Whenever a first responder determines that a biological threat may be present, he or she should **immediately call the FBI** Field Office and ask to speak to the Weapons of Mass Destruction (WMD) coordinator. The FBI website is http://www.fbi.gov.

The FBI WMD coordinator will respond to the scene and will, in conjunction with other federal, state, local, and internal experts, conduct a threat assessment to determine the credibility of the threat. FBI, as Lead Federal Agency for crisis

management, will tailor the response to the level of threat. If the threat appears credible, the FBI will take appropriate steps that match the threat including:

- Site assessment;
- Arranging for definitive testing at one of the Laboratory Response Network (LRN) laboratories;
- Arranging for or coordinating appropriate packaging, chain of custody procedures and transportation of samples to the laboratory;
- Informing public health, hazmat, and other local authorities about the situation;
- Notifying the U. S. Postal Inspection Service, whenever it appears that the threat was delivered through the U. S. Postal Service, and then ensuring that origin and tracking information is obtained from the mail piece (ideally, digital photographs of the front and back);
- Identifying and listing the names of anyone who may have been exposed to the suspicious substance;
- Asking all potentially exposed persons to wash their hands.

Bombs, dangerous chemicals, and radiological threats, by their very natures, require immediate, crisis-level responses. Biological agents, on the other hand, may not make people sick instantaneously. Most biological weapons have an incubation period, which ranges from 3 to 7 days. Results will usually be available from the LRN laboratory in about 2 days, so there will be enough time to form and coordinate an appropriate response, including treatment when appropriate, before symptoms appear. Dramatic steps such as closing large buildings are not appropriate until the LRN results have been received.

In the event that microbiological culture in an LRN laboratory produces a positive result, decisions regarding quarantine and treatment of potentially exposed individuals must be made as an integrated process involving local public health, law enforcement, hazmat first responders, and local federal management. Preplanning, training, and rehearsal are essential to making this work. The process for responding in these circumstances is laid out in detail in the Technical Assistance for Anthrax Response" issued by the National Response Team (www.nrt.org).

Communications: Occupational Safety and Health Administration (OSHA) standards require employers to make health and safety information available to any employee who requests it. As discussed above, all information relevant to apparent and credible biological threats should be provided to employees as quickly as possible, preferably without waiting for a request. Health and Safety Plans, also required by OSHA regulations, must include provisions for sharing health and safety information.

Record keeping: Federal agencies must keep careful and complete records of all apparent biological threat events, including all advice received from first

responders, law enforcement, and public health officials, and the specific content of any information conveyed to employees and the public.

Chain of evidence protocol requires that a name, date, time, and signature be obtained every time custody of a suspicious material or sample for laboratory analysis changes hands.

Decontamination: The level of decontamination effort depends on the credibility of the threat. If a competent authority has determined that the threat is not credible and not a criminal hoax, then a simple cleanup is sufficient, using any appropriate household or industrial cleaning agent.

In the case of a credible threat, the material should not be cleaned up. It is important to make sure that enough material remains for:

- Laboratory analysis, if necessary;
- Use as criminal evidence, regardless of whether the threat is ultimately determined to be infectious, toxic, or simply a criminal hoax.

U. S. Postal Service regulations do not require that a mail center deliver every piece of mail. Mail is occasionally contaminated with noxious materials that are not otherwise hazardous. Once these guidelines have been followed to their conclusion, federal mail centers are free to dispose of mail as they see fit.

Of course, if a threat proves to be real, the Environmental Protection Agency, local public health authority, and many others will have to be involved in the cleanup and decontamination.

Irradiated Mail: The USPS is irradiating much of the mail that is being delivered to federal agencies in the Washington DC, metropolitan area. This should be considered in the site assessment phase carried out by the first responder. The risk to workers would be lessened if the biological agent has been destroyed by irradiation. The threat, if credible, still would be referred to the FBI.

VI. Sampling, testing, and sanitization

Vendors seeking to sell a wide variety of measures to monitor, test, and sanitize the mail frequently contact federal mail managers. All available scientific evidence indicates that the following are inappropriate for routine use in mail centers for assessing or managing any type of biological threat:

- Hand-held immunoassay devices
- Polymerase Chain Reaction (PCR) rapid field tests
- Autoclaves

- Ultra-violet treatment
- Ethylene oxide treatment
- "Sniffers"
- Routine sampling
- Routine culturing of samples
- Quarantining mail pending the results of routine sampling and testing.

GSA recommends, therefore, that these devices and processes not be used in federal mail centers or by first responders to federal mail centers.

Please note that this recommendation applies only to *routine use in federal mail centers.* Some of these technologies are entirely appropriate for use in other situations, including:

- Assaying or cleanup of actual biological attacks;
- Research and development that may lead to development of assay devices or treatments that are appropriate for mail center use in the future;
- Development of devices for use in military situations;
- U. S. Postal Service mail processing facilities; or
- Defined, high threat situations, where a scientifically validated technology platform is selected and installed as part of a carefully developed concept of operations, including consequence management that fits the technology.

The Department of Health and Human Services (DHHS) has released guidance on use of these methods indicating that the effectiveness of these methods is unsatisfactory. A copy of this guidance is attached as Appendix E.

On this issue, Dr. John H. Marburger, Director, OSTP, signed a memorandum on July 19, 2002, which included the following statement:

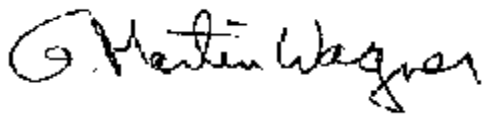
> "Until further notice, the Office of Science and Technology Policy advises that federal agencies cease issuing any new procurement requests, task orders, purchase orders, or contracts for the purchase of new equipment or services that may detect, sample, test or filter air for *Bacillus anthracis* as the method for assaying suspicious mail, or for routine environmental sampling of mail rooms. The Department of Defense will continue to procure military standard biological detection equipment following the current statutory regulations under which the Department operates. "

Dr. Marburger's memorandum remains in effect. To view the entire memorandum, see Appendix F.

Summary

Since September 11, 2001, all levels of government have cooperated to strengthen our nation's security and defend against terrorism. The United States Postal Service (USPS) has instituted a number of procedural changes to minimize the threat to their workers and mail center workers across the United States. The most critical of these is cleaning high-speed mail processing equipment with HEPA-equipped vacuum cleaners instead of blowers.

Together, these changes have established a reasonable level of protection for mail center workers. Solid, believable information gives people the confidence to make informed choices, and informed choice gives a sense of control over our destiny. The Interagency Working Group has designed this document to help federal agencies perform their critical missions for the American people.



G. Martin Wagner
Associate Administrator

Appendixes

- A –Working Group Members
- B – Additional Considerations of Preparing
- C – Standard List of Suspicious Characteristics (FBI)
- D – Useful Websites
- E – Statement By the Department of Health and Human Services
- F – Memo from Dr. Marburger

Appendix A: Working Group Members

The members of the Interagency Working Group that prepared these guidelines represent the:

Department of Defense
- Program Executive Office for Chemical/Biological Defense Command (CBDCOM)
- U.S. Army
- U.S. Military Postal Service Agency

Department of Energy
- Lawrence Livermore National Laboratory

Department of Health and Human Services
- Office of the Secretary for Public Health Preparedness

Department of Homeland Security (DHS)
- Federal Protective Service
- Science and Technology Directorate

Department of Justice
- Federal Bureau of Investigation

Department of Treasury
- Internal Revenue Service

Environmental Protection Agency (EPA)

General Services Administration (GSA)
- Office of Governmentwide Policy
- Public Buildings Service Chicago

New York State Department of Health

Office of Science and Technology Policy (OSTP)

U.S. Postal Service

Appendix B: Additional Considerations in Preparation

Mail center design: All but the smallest mail centers should be placed in enclosed, dedicated rooms, with controlled access and limited points of entry. If possible, mail centers should be located near loading docks. This will allow the mail to travel directly to the mail center from the outside and reduce the impact that any potentially contaminated mail will have on the rest of the building. Wherever the volume of mail, the security assessment, and a cost-benefit analysis make it appropriate, the mail center should have its own air handling and ventilation system, including High Efficiency Particulate Air (HEPA) filters, and procedures for shutting down ventilation. A HEPA filter system reduces, and in some instances may eliminate bacteria in the environment; it will also control the paper dust that is inherent in handling mail.

Nonporous materials should be used to construct and furnish the mail center. For example, tile floors should be used instead of carpeting, and hard plastic or metal furniture should be installed instead of fabric-covered furniture. Gloss or semi-gloss paint should be used on all painted surfaces. A lighting level of 100 foot-candles is recommended to assist personnel in identifying suspicious mail. A telephone should be installed within the mail center, where possible, so personnel can contact the proper individuals when necessary.

Disabled employees: Every federal agency must provide a safe working environment for all employees, including those with special needs. Security procedures should specifically address communications with Individuals who may need assistance during an emergency. Additional information on emergency preparedness for disabled employees can be found at the web site of the National Organization of the Disabled at http://www.nod.com.

Contractors: Contracts for mail center operations or related functions should specify security procedures that the contractor and contract personnel must follow.

Gloves, masks/respirators, and protective clothing: Gloves and respirators (masks) should be made available, but not required, for any mail center workers or others who process mail, because wearing gloves or a respirator eases the fears of some workers. Other protective clothing is unnecessary except to protect workers' clothing from dust and other dirt. Where respirators are used, a written respiratory program must be established that conforms to the requirements of OSHA's respiratory protection standard as specified in 29 CFR 1910.134(c)(2). See http://www.osha.gov.

The Laboratory Response Network for Bioterrorism (LRN) is a network of governmental (local, state and federal laboratories that have been trained by the

Centers for Disease Control and Prevention (CDC) to process samples by well-established and validated procedures. These laboratories utilize LRN standard protocols for testing and must successfully complete periodic proficiency testing challenges sent from the CDC. The LRN was formed as a self-organized group through the efforts of the CDC and the Association of Public Health Laboratories (APHL). Through the APHL, local, state, national and global health leaders are linked to promote the highest quality laboratory practices worldwide.

To identify the appropriate LRN laboratory when developing the security plan, call the APHN at 202-822-5227.

FBI Advisory

If you receive a suspicious letter or package

What should you do?

1. Handle with care
   Don't shake or bump
2. Isolate and look for indicators
3. Don't Open, Smell or Taste
4. Treat it as Suspect!
   Call 911

If parcel is open and/or a threat is identified. . .

For a Bomb

Evacuate Immediately
Call 911 (Police)
Contact local FBI

For Radiological

Limit Exposure - Don't Handle
Distance (Evacuate area)
Shield yourself from object
Call 911 (Police)
Contact local FBI

For Biological or Chemical

Isolate - Don't Handle
Call 911 (Police)
Wash your hands with soap and warm water
Contact local FBI

Police Department _____

Fire Department _____

Local FBI Office _____

(Ask for the Duty Agent, Special Agent Bomb Technician, or Weapons of Mass Destruction Coordinator)

GENERAL INFORMATION BULLETIN 2000-3
Produced by: Bomb Data Center
Weapons of Mass Destruction Operations Unit

Appendix D: Useful Websites

Bureau of Alcohol, Tobacco and Firearms (BATF) – www.atf.treas.gov

Centers for Disease Control and Prevention (CDC) - www.bt.cdc.gov

Council on Foreign Relations - Homeland Security Questions and Answers on Biological Attacks - www.cfrterrorism.org/security/

Department of Homeland Security – www.Whitehouse.gov/homeland or www.dhs.gov/dhspublic/

Federal Bureau of Investigation (FBI) – www.fbi.gov

Federal Emergency Management Agency (FEMA) – www.fema.gov

Federal Protective Service - www.dhs.gov/

General Services Administration (GSA) – www.gsa.gov

GSA Mail Communications Policy Office - www.gsa.gov/mailpolicy

Office of Personnel Management - publishes questions and answers on federal employees personnel issues, etc. - www.opm.gov

U.S. Department of Labor (DOL), Occupational Safety and Health Administration (OSHA) - www.osha.gov

U.S Postal Service (USPS) – www.usps.com

USPS Postal Inspection Service - www.usps.com/postalinspectors

Workplace Risk Pyramid, OSHA - www.osha.gov/bioterrorism/anthrax/matrix

Appendix E

STATEMENT BY THE DEPARTMENT OF HEALTH AND HUMAN SERVICES
Regarding Hand-Held Assays for Identification of *B. Anthracis* Spores

Purpose
To provide law enforcement, fire services, emergency managers and other first responders with guidance regarding the purchase and use of hand-held assays used for detecting anthrax spores and other biological agents.

Summary

The U.S. Department of Health and Human Services at this time recommends against use by first responders of hand-held assays to evaluate and respond to an incident involving unknown powders suspected to be anthrax or other biological agents.

Background
In recent months, Federal, State and local first responders have had to evaluate numerous samples of white powdery substances to determine if B. anthracis (anthrax) spores are present. In some cases, field tests showed an apparent "positive" result and this led to the quarantine, isolation or decontamination of people. When these samples were referred to a reference lab in the Laboratory Response Network (LRN), they were found to be negative through microbiological culturing and molecular methods. The devices used for the initial field tests included tickets and strips from at least four vendors. Problems resulted from a variety of factors, such as testing of caustic or harsh chemicals or the performance of tests by inadequately trained personnel.

Discussion
Biological agent field test kits are, at this time, not sufficiently accurate for on-scene decision making in the field. Besides the high number of false positive results, hand-held assays also yield negative results on samples that are truly positive (false negatives). In formal terms, the sensitivity of such assays are in the range of 100,000 spores whereas a culture may detect one spore.

In contrast to situations with chemical exposure where rapid decision making (minutes) can be crucial to the protection and treatment of individuals, there are no examples of biological exposure where decision-making cannot wait for the results of validated laboratory procedures (1-2 days). Any perceived benefit of using currently available hand-held assays fall short of the costs of unnecessary remedial actions and amplified public concern.

No Federal agency certifies or approves these devices. The FBI and CDC have recently evaluated commercially available hand-held assays for the detection of B. anthracis. These studies confirm the low sensitivity of such assays and their potential to produce

false-positive results with non-anthrax bacteria and chemicals. The performance of handheld assays for the detection of biological agents other than B. anthracis has not been evaluated and their use is also not recommended at this time.

Conclusions

Until results are obtained that would warrant the use of hand-held assays, DHHS recommends:

(1) hand-held assays systems not be used for the assessment of suspected biological samples;
(2) Whenever a biological agent is suspected, a unified command should assess the credibility of the situation and determine an appropriate response. The unified command should include fire services, public health, the FBI's Weapons of Mass Destruction Coordinator, and law enforcement;
(3) Substances that are found to be a credible public health threat by the unified command should be screened in the field for volatile organic compounds (VOC), pH, explosives, and radiation, and then sent to an appropriate laboratory in the Laboratory Response Network (LRN) for testing. First responders and local public health programs need to establish protocols to provide this support and logistics of the response. Besides testing of samples in an LRN laboratory, the protocol should include a system for identification and follow-up of the potentially exposed population and a joint communication plan for the public and media relations. Since exposure to airborne anthrax spores is potentially life threatening, all credible threats should be handled appropriately in a timely manner.

References:

1. "CDC Health Advisory: Hand-Held Immunoassays for Detection of Bacillus anthracis Spores." October 18, 2001 http://www.bt.cdc.gov/DocumentsApp/Anthrax/10182001HealthAlertPM/10182001HealthAlertPM.asp
2. "Use of Onsite Technologies for Rapidly Assessing Environmental Bacillus anthracis Contamination on Surfaces in Buildings." CDC MMWR Vol 50 Number 48. December 7, 2001. http://www.cdc.gov/mmwr/PDF/wk/mm5048.pdf
3. "Approved Tests for the Detection of Bacillus anthracis in the Laboratory Response Network." http://www.bt.cdc.gov/DocumentsApp/Anthrax/ApprovedLRNTests.asp

Appendix F: Memorandum from Dr. John H. Marburger, III