HSDailyWire.com
THE BUSINESS OF HOMELAND SECURITY

Guest column

The government's new mail room

How CRF regulations overhaul mail security -- and the keys to timely compliance

// by Keith James
28 May 2009

The recent rise in white powder hoaxes and mail security breaches is taking its toll -- and for the government, enough is enough: Come 25 August, how federal agencies safeguard employees, mail rooms, and overall facilities face drastic changes.

All federal mailrooms, regardless of size, staffing, or operational capacity -- whether in an office building in Washington, D.C., or a Coast Guard vessel patrolling the Atlantic -- must implement and maintain a comprehensive security policy meeting several federal standards. Most agencies fall far from compliance today, and face just weeks to overhaul existing processes. This means a lot of scrambling -- and implementation of security protocols and technology -- to get checklists up to speed.

Created in response to provisions outlined in Homeland Security Presidential Directive HSPD-7 Federal, the requirement amends the Public Contracts and Property Management title of the Code of Federal Regulations (CFR) to reflect the heightened state of awareness necessary to safeguard federal postal and shipping facilities.

The regulation, located under Title 41 §102-192 sections 70-80, outlines the specific policies that need to be met, as well as the various elements associated with developing, implementing and sustaining a security plan that meets compliance.

The key takeaways

- Each agency must establish and maintain a mailroom-specific security policy, and develop a facility-centric security plan commensurate with the size and responsibilities of each facility
- All federal mail programs must identify, prioritize and coordinate the protection of each mail processing facility against both internal and external security threats

A Multi-tiered approach to compliance

Meeting these complex regulations, and developing a comprehensive safety plan, cannot happen overnight. Several steps need to be taken:

Conducting facility-based assessments. This is the first step toward compliance. These evaluations weigh the overall level of risk of a specific location -- and determine the most effective way to implement the requirements needed to protect facility staff and visitors. Each assessment must equally focus on identifying the widest range of threats, and consist of continuous internal evaluations and annual external reviews.

Developing and implementing security related operating procedures and mail screening protocols. Designed to protect personnel, these procedures safeguard facilities and provide direction for managing a variety of threat scenarios including biological, chemical, radiation, explosive, and natural and man-made disasters. These also need to account for today's most disruptive threat scenarios -- mail hoaxes -- which continue to consume growing costs, resources, and time from first responders and law enforcement.

Rigorous employee training: Agencies should develop minimum training requirements which, when tailored to the facility level, address all major aspects of threat prevention, recognition, and detection. The plan should clearly delineate each person's role and provide a clear understanding of the security plan.

In addition, multi-layered plan testing and rehearsals, comprising various levels of tabletop walkthroughs and real time drills, must play a key role. Focused on specific events, these should bring together internal and external support elements including mailroom managers, facility engineers and managers, and external first responders.

Developing a communications plan. This handles internal and external communication requirements, identifying each mailroom manager's responsibilities within a full range of potential threats. It also identifies the primary and secondary communication methods, protocols and strategies.

Instituting an Occupant Emergency Plan (OEP). These are specifically designed to safeguard and account for individuals in the event of an incident. Because the mailroom is so often a part of a larger facility or organization, its OEP must meet agency and facility requirements. Mailroom managers must coordinate information about the day-to-day collection and sharing of methodologies with the facility security manager. The plan must take into account each and every member of the team.

Establishing a Continuity of Operations Plan (COOP). These address post-event actions designed to enable resuming operational activities -- as quickly and efficiently as possible. The plan normally covers long- and short-term operational support requirements, and requires a great deal of pre-event coordination, rehearsal, and training. They need to be reviewed and tested annually to ensure they still meet primary program objectives.

Technology paves the fast path to compliance

While the development of these various security plans and policies require several human-based processes, technology plays a prominent role in upholding these

standards, maintaining continual compliance and preserving the highest safety standards.

Specifically, some of the tools -- such as chemical, biological, radiological, nuclear, and explosive (CBRNE) detectors - are highly technical, while some are as low-tech as simple occupant tracking systems and building visitor logs which allow for the rapid accounting of personnel in the event of an emergency. Video document access and general video monitoring can monitor specific activities, minimizing both internal and external threats.

Dedicated radios that do not interfere with or depend on cell phone technology are especially effective when traditional circuits are interrupted or jammed due to over use. Cell phones should never be relied on as a primary communications method. In large scale emergencies, these circuits rapidly become jammed as dozens of individuals call family members, friends, or as is all too often the case today, the media.

Buildings' internal communications systems can function to readily alert all personnel of an emergency. Other technology advances include mobile mail centers used as part of an agency's COOP, and monitored communications technology used to support and enhance a communications security plan.

The reality is that most agencies do not house the internal expertise or skills to develop and execute these advanced security requirements, which is resulting in more agencies turning to external assistance to strike compliance. While mail and facility managers can participate actively in the development and implementation of the overall program, engaging in the service of experienced outside mail security professionals can simplify the process, speed compliance -- and minimize all the scrambling that will be a common occurrence in mail rooms across the country in the coming weeks.

Keith James is a Senior Program Director for SoBran, Inc. in Fairfax, Virginia, specializing in mail stream security. SoBran provides mail screening and security related services to a wide range of governmental agencies and commercial clients. For more information on this or other security related compliance issues please contact SoBran at 703.352.9511.