STEP BY STEP TO FACILITY SECURITY

Maintenance of safety in the ECC is a prerequisite for public safety.

By Stephen Martini, ENP, RPL

Are you safe while you are busy keeping your citizens and responders safe?

The emergency communications center (ECC) is always front of mind when preparing for or mitigating against an attack. Chaos inside the ECC can magnify chaos in the community. Whether planning against a terror threat or natural disaster, the security of your facility is essential to maintaining continuity of operations.

A few guiding documents exist to help you prepare. If you're seeking new construction or renovation of an existing space, give some attention to the following resources. If neither activity is on the horizon, review these opportunities for improvement during your next continuity of operations plan review.

NFPA 1221[1]

This National Fire Protection Association standard is specific to the installation, maintenance and use of emergency communications

> **We operate in a 24/7 environment, which means adequate staff is required to facilitate our badge management program for visitors and provide an escort when necessary.**

systems. In chapter four it describes how ECCs should be built to protect against hazards. Section 4.6 speaks to facility security, requiring ECCs to be:

- Protected against damage from vandalism, terrorism and civil disturbances.
- Restricted for access to authorized individuals.
- Protected with bullet resistant doors boasting a fire-resistance rating of at least one-hour, exterior windows that cannot be opened and external walls.[2] (Specific guidance exists for facilities without bullet-resistant exterior windows.)
- At least 82 feet (25 meters) from access by unauthorized vehicles (or closer if the building is blast resistant).
- Monitored by electronic intrusion alarms at points of potential unauthorized entry, with an audible announcement made in the operations room.
- Protected by a security vestibule.

APCO ANSI STANDARD 2.103.1-2019 PUBLIC SAFETY GRADE SITE HARDENING REQUIREMENTS[3]

This standard features guidance on physical security as well. It states, "security includes asset protection, threat assessment, threat detection, and threat containment … including theft, vandalism and malicious intent to impair the assets and/or the system." The standard acknowledges that risks do not apply equally to different site types, especially for those located in urban, suburban or rural environments, focusing heavily on the construction of fencing and gates to protect the perimeter and restrict public access. Fences and gates serve a variety of purposes, including warning casual observers of access restrictions, deterring access to the site, delaying those who may actually access the site and establishing criminal intent for those who attempt to cross. Fences

should be constructed to specific minimum standards regarding materials used, height and placement. Gates should be built to a similar or higher quality standard. The fence should feature signage around the entire property. Additionally, the standard speaks to security around cables, wires, feed lines, radio antennas, on-site fuel storage, generators and other power sources.

SECURITY BEYOND PHYSICAL CONSTRUCTION

When considering man-made threats, your agency should include security measures that go beyond physical construction. Access controls and surveillance devices, including internal and external security cameras, provide broad visibility to facility and property. In line with visibility, proper distance creates secure areas between public access points and mission-critical spaces.

Controlling access to those spaces can be done, efficiently and easily, with an employee badging system. Badges (also called key cards) can be used to allow or restrict access to certain areas of your property or facility either by role (job title) or individual. Employees should each have an access badge, complete with photo identification updated often enough to reflect the current likeness of the badge holder.

Industry partners or maintenance professionals may also need to access your facility or property from time to time, which requires credentialing, an access badge checked in and out by a team member tasked with managing facility access, and, depending on their destination, an escort. We operate in a 24/7 environment, which means adequate staff is required to facilitate our badge management program for visitors and provide an escort when necessary.

When placing badge access readers within your facility, look for opportunities to create

a sally port concept, fortifying interior spaces from exterior entry points. Elevators and stairwells should require badge access to obtain entry to interior doors or additional floors. These access points should create layers of barriers between bad actors and your most important production environment and people.

Consider the security needs of your location, both at noon and midnight. Is there adequate lighting in all areas and at all entry and exit points? Is access impeded or assisted in all types of weather? A snowdrift against an exterior wall may prove to be an effective ladder in March that is not there in July. Consider the impact of a power outage at your facility. How do automatic door locks function in the event of a power failure? What might you need to put in place to secure doors that may become unsecured during a blackout?

If a threat level increased, what actions might you take to ensure facility security? Think through those scenarios, identifying the weak points around an escalating threat – perhaps a crowd of violent protestors swelling around the perimeter fence – then consider what actions you may need to take

> **"When planning a secure facility, consider your personnel as a critical resource. ECC employees are the first and last point of defense against those with malicious intent.**

now to minimize the need for further escalation later.

PERSONNEL ARE KEY TO FACILITY SECURITY

When planning a secure facility, consider your personnel as a critical resource. ECC employees are the first and last point of defense against those with malicious intent. Employees should pay attention to those in or around the building and politely engage with unfamiliar people to determine who they are, their reason for visiting and whether they are in the right location. Employees have a responsibility to prevent tailgating or piggybacking when an unauthorized person

follows a credentialed person into a secure area without their knowledge or consent. Though it may feel rude to allow a door to close on a co-worker or a stranger, it is imperative that personnel use their own credentials to access secure areas every time. Was that individual terminated overnight, with access credentials revoked? A disgruntled co-worker or ill-intentioned former vendor can wreak havoc in an ECC if an over-trusting team member allows access to a secure area.

Additionally, we must ensure our personnel receive regular training on this topic in the same way we mitigate against cyber threats. Personnel should train to control and protect material and manage and control access to the property and facility.

Finally, all considerations you give to your primary facility must also be given to an alternate or backup facility.

To help your agency comply with these standards, the Federal Emergency Management Agency offers a helpful checklist to assess the readiness of emergency operations centers,[4] which can also apply to the ECC. ●

Stephen Martini, ENP, RPL, is Director at Metro Nashville Emergency Communications Center.

REFERENCES

1. Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems. National Fire Protection Association. 2019. https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1221

2. Standard for Bullet-Resisting Equipment. UL Standard. https://standardscatalog.ul.com/ProductDetail.aspx?productId=UL752

3. ANSI 2.106.1 Public Safety Grade Site Hardening Requirements. APCO International. 2019. https://www.apcointl.org/download/public-safety-grade-site-hardening-requirements/

4. "National Engagement for Draft Emergency Operations Center (EOC) How-To Quick Reference Guide." Federal Emergency Management Agency. www.fema.gov/sites/default/files/documents/fema_eoc-how-to-quick-reference_guide_0.pdf

CDE EXAM #58176

QUIZ

1) APCO, FEMA and NFPA provide guiding documents to assess and resolve your agency's facility security concerns.
   a. True
   b. False

2) Which section of NFPA Standard 1221 specifically addresses facility security?
   a. 1.3
   b. 2.1
   c. 3.9
   d. 4.6

3) ECCs should plan to protect their facilities against vandalism, terrorism and which other man-made threat?
   a. Balloon animals
   b. Tornados
   c. Civil Disturbances
   d. Earthquakes

4) Which three things should be both fire and bullet resistant?
   a. Doors, interior windows and external walls
   b. Doors, exterior windows, and external walls
   c. Doors, roofs, and floors
   d. Interior windows, roofs, and doors

5) How close should unauthorized vehicles be allowed to get to the ECC facility?
   a. 82 feet (25 meters)
   b. 64 feet (19 meters)
   c. 21 feet (6 meters)
   d. 90 feet (27 meters)

6) All ECCs should be protected by a security vestibule.
   a. True
   b. False

7) The APCO ANSI Standard related to Public Safety Grade Site Hardening Requirements states threats include theft, vandalism and which other concern?
   a. Rain
   b. Criticism
   c. Overuse
   d. Malicious intent

8) Which of the following is *not* a benefit of adding a fence around the ECC facility?
   a. It prevents anyone from ever accessing your facility without approval.
   b. It warns casual observers of access restrictions.
   c. It deters those attempting to access the site.
   d. It establishes criminal intent for those who do attempt to cross.

9) Following a credentialed person into a secure area without their knowledge or consent is called:
   a. Highlighting
   b. Shim-Shamming
   c. Boot-Scooting
   d. Tailgating/Piggybacking

10) Who are the first and last line of defense against protecting the ECC facility from people with malicious intent?
   a. ECC employees
   b. Visitors to the ECC
   c. Contracted security officers
   d. Consulting firms

FOR CREDIT TOWARD APCO RECERTIFICATION(S)

Each CDE article is equal to one credit hour of continuing education

1. Study the CDE article in this issue.

2. Answer the test questions online (see below for online exam instructions) or on the exam page from the magazine article (photocopies are not required).

3. Add/upload your CDE article information and certificate of achievement in the "My Classes Taken" section of APCO's Training Central at www.apcointl.org/trainingcentral.

Questions? Call us at (386) 322-2500.

You can access the CDE exam online!
To receive a complimentary certificate of completion, you may take the CDE exam online. Go to http://apco.remote-learner.net/login/index.php to create your username and password. Enter CDE in the search box, and click on the "2021 Public Safety Communications Magazine Article Exams," then click on "enroll me" and choose "Facility Security **(58176)**" to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.