

Comments on National Fire Protection Association (NFPA) 3000 Standard for an Active Shooter/Hostile Event Response Program (ASHER)



Contents of Comments on NFPA 3000

Table of Contents

Introduction	2
Industry Impact Key	3
Chapter 3 Definitions	4
Chapter 4 ASHER Program Development Process.....	7
Chapter 5 Risk Assessment	8
Chapter 6 Planning/Coordination	10
Chapter 7 Resource Management.....	12
Chapter 8 Incident Management.....	13
Chapter 9 Facility Preparedness.....	14
Chapter 10 Financial Management	16
Chapter 11 Communications Center Support.....	17
Chapter 12 Competencies for Law Enforcement Officers.....	18
Chapter 13 Competencies for Fire and Emergency Medical Services (EMS) Responders.....	19
Chapter 14 Personal Protective Equipment (PPE)	20
Chapter 15 Training	21
Chapter 16 Public Education	22
Chapter 17 Public Information.....	23
Chapter 18 Continuity of Operation.....	25
Chapter 19 Hospital Preparedness and Response for Out-of-Hospital ASHER Incidents	26
Chapter 20 Recovery	29
Annex A Explanatory Material.....	30
Annex B Laws, Regulations, Consensus Standards and Guidance Documents.....	32
Annex C Informational References.....	33

Comments on NFPA 3000 Standard for an ASHER Program

Introduction

The security and public safety industries have seen a significant number of standards and guidelines introduced in response to active shooter events. Although global events occur in greater frequency and incorporate differential assailant methods, most of the industry guidance has originated in North America.

Recently the [Security Industry Association \(SIA\)](#) has introduced the [Partner Alliance for Safer Schools \(PASS\)](#), bringing together representatives of the security industry, law enforcement and educational institutions to gather, develop and make publicly available information about securing schools, establishing a tiered framework for school security solutions¹. SIA has also introduced both public safety and autonomous systems working groups, helping public/private partnerships work with interoperable domain awareness solutions.

NFPA recently introduced its first provisional standard, [NFPA 3000, Standard for an ASHER Program](#). Created with insight from multiple public safety and first responder disciplines such as fire, EMS and law enforcement, NFPA 3000 aims to provide advanced reaction guidance to a hostile event through unified planning, response and recovery.

Why a provisional standard? This gives the NFPA, a standards developer accredited by the American National Standards Institute, the opportunity to conduct ongoing research improving this “voluntary consensus standard.”

The 80-page standard was developed by a committee of members from private industry, subject matter experts on training and disaster recovery, emergency managers and federal, state and local law enforcement personnel. Many hostile and mass casualty events were considered in creating minimum criteria for the level of competence required to manage, organize and sustain an active shooter or hostile event preparedness and response program.

Different terminology is used across multiple standards development organizations (SDO) like NFPA, SIA and ASIS International: an active assailant may refer to both an active shooter and an individual or group involved with a hostile event. As it was shown in the November 2015 Paris attacks, different modes of attack can be used, and practitioners must consider the most relevant guidance for their requirements.

The following is a review offering opinion on industry impact, with consideration for supplemental references that may be considered. The practitioner should consider multiple perspectives and a wide range of detection systems when developing preparedness, response and recovery.

1 [“PASS,” Security Industry Association, web.](#)

Industry Impact Key

A review of NFPA 3000 Standard for an ASHER Program shows there is relevance to the electronic physical security industry. While most of the recommendations included in the standard are low impact, there are some key areas where attention must be paid based on an organization's security industry context.

Chapter	Industry Impact
Chapter 3 Definitions	Medium/High
Chapter 4 ASHER Program Development Process	High
Chapter 5 Risk Assessment	High
Chapter 6 Planning/Coordination	High
Chapter 7 Resource Management	Low – Informative
Chapter 8 Incident Management	Low – Informative
Chapter 9 Facility Preparedness	High
Chapter 10 Financial Management	Low – Informative
Chapter 11 Communications Center Support	High
Chapter 12 Competencies for Law Enforcement Officers	Low - Informative
Chapter 13 Competencies for Fire and EMS Responders	Low – Informative
Chapter 14 Personal Protective Equipment (PPE)	Low – Informative
Chapter 15 Training	Low – Informative
Chapter 16 Public Education	Low – Informative
Chapter 17 Public Information	High
Chapter 18 Continuity of Operation	Medium
Chapter 19 Hospital Preparedness and Response for Out-of-Hospital ASHER Incidents	Medium
Chapter 20 Recovery	Low – Informative

Chapter 3 Definitions

Reference: 3.3.2 – 3.3.5, Definitions of Active Assailant, Active Shooter, ASHER and ASHER Program

The U.S. Department of Homeland Security (DHS) defines an active shooter as “an individual actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearms and there is no pattern or method to their selection of victims.” This is consistent with NFPA 3000.

However the term “active assailant” in NFPA 3000 refers to devices or means other than firearms. This is where terminology may differ. In addition to [numerous state government programs](#)², the [International/National Academies of Emergency Dispatch](#)³ and several insurance providers use the term “active assailant” to *include* the use of firearms and an active shooter scenario.

One leading industry communications provider for mass notifications and critical communications in emergencies on corporate or school campuses makes the case for the term as inclusive rather than exclusive:

“An ‘active assailant,’ which is a person (or group of persons) actively engaged in killing or attempting to kill or cause serious bodily injury to a person or group of persons. The weapon could be a gun, or it could be something else, such as a knife, explosive device or car. The key difference between ‘active shooter’ and ‘active assailant’ is that the weapon is not specified. As threats continue to expand, the ‘[active assailant](#)’ term is perhaps more accurate and more appropriate⁴.”

The Occupational Safety and Health Administration, under safety and health topics, makes reference to the implementation of a workplace violence prevention program, rather than the specific reference of “active shooter.”

Due to a worldwide increase in firearm- and non-firearm-based attacks (including those with vehicles, explosives, incendiary devices, stabbings, slashing and acid attacks), some global agencies are now encouraging the use of the more general descriptor “mass casualty attacker.”

*Industry Impact: **Medium***

Supplemental Standards and Guidelines: Also see footnotes:

- [“Active Assailant Exercise Design Series,”](#) Everbridge, web:
- [“White Paper for the Integrated Public Safety Response to the Active Shooter/Active Assailant,”](#) The North Carolina Active Assailant and Mass Violence Work Group and The North Carolina Department of Justice, Aug. 2, 2017, web.

2 [“White Paper for the Integrated Public Safety Response to the Active Shooter/Active Assailant,”](#) The North Carolina Active Assailant and Mass Violence Work Group and The North Carolina Department of Justice, 08/02/2017, web.

3 [“Active Assailant \(active shooter\) Protocol 136,”](#) The International/National Academies of Emergency Dispatch, 2018, web.

4 [“Active Assailant Exercise Design Series,”](#) Everbridge, web.

- [“Active Assailant \(active shooter\) Protocol 136,”](#) The International/National Academies of Emergency Dispatch, 2018, web.

Reference: 3.3.14, “Communications Center”

In many cities, this is co-located with the emergency operation center (EOC), especially those with Next Generation 911 centers.

Industry Impact: Medium

Supplemental Standards and Guidelines:

- [“National Emergency Number Association \(NENA\) Communications Center/PSAP Disaster and Contingency Plans Model Recommendation,”](#) web.
- [“NENA Drills and Exercises Information Document,”](#) web.
- [“NENA Operational Impacts of Devices and Sensors Information Document,”](#) web.
- [“NENA Master Glossary of 9-1-1 Terminology,”](#) web.

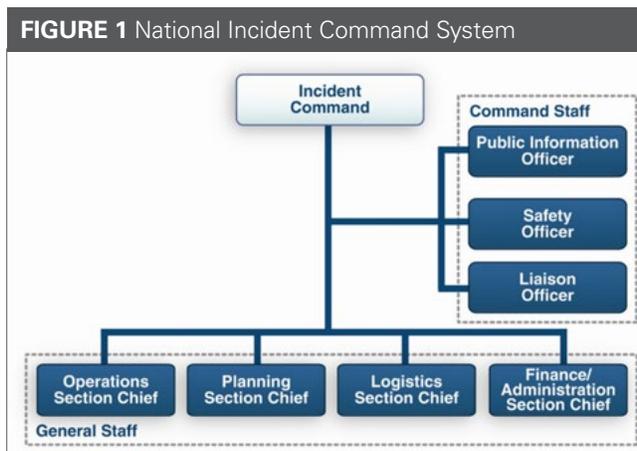
Reference: 3.3.26 “EOC”

The EOC reference could be reworded to support “incident command,” the field operations center that is “stood up” and is connected to the EOC and other elements of the command structure.

Supplemental Standards and Guidelines:

Since the EOC is a vital focal point of multiagency coordination systems (MACS)/EOC, an overview of key National [Incident Management System \(NIMS\) principles](#) relating to MACS, public information, resource management, mutual aid and communication and information management is required⁵.

According to training established by the Federal Emergency Management Agency (FEMA) Emergency Management Institute (EMI), NIMS Training Program, Incident Command System Resource Center, it is important to effectively manage and operate EOCs and multiagency coordination systems at the federal, state, tribal and local levels of government. [This definition should be expanded](#) to describe the role, design and functions of EOCs and their relationships as components of a multiagency coordination system⁶.



Credit: National Incident Management System (NIMS), US Department of Homeland Security, Dec. 2008

5 [“Incident Command System \(ICS\) Glossary,”](#) Incident Command System Training, web.

6 [“Incident Command System Training,”](#) FEMA EMI, National Incident Management System (NIMS) Training Program, Incident Command System Resource Center, web.

Roles in the NIMS are outlined in the document "[Planning and Triage in the Disaster Scenario](#)"⁷; American Academy of Pediatrics."

Industry Impact: **Medium**

Reference: 3.3.25, "Electronic Premises Security System"

This is referred to in NFPA 3000 as "components and circuits to monitor or control activity or access to a protected premises system."

To be consistent with the terminology used in the security industry, "Electronic Premises Security System" is usually four systems: video surveillance, perimeter and/or intrusion detection, electronic access control and a building openings/door locking hardware system.

Although it is a clarification in terminology, the importance of both the facility practitioner and the first responder being aware of individual electronic safety and security resources is high. A video surveillance system can provide improved situation awareness of where students or employees are exiting a building or taking refuge. A perimeter intrusion detection system can report unusual activity after hours. The electronic access control, together with door locking hardware, can maintain life safety through free egress, while providing valuable functions like emergency lockdown, free egress or employee trace.

Industry Impact: **High**

7 "[Planning and Triage in the Disaster Scenario](#)," American Academy of Pediatrics, web.

Chapter 4 ASHER Program Development Process

Reference: NFPA 3000 4.2, States “Facility Preparedness in Accordance with Chapter 9”

Chapter 9 Section 9.3.7 notes the following:

- Facility assessment to support preparedness, protective actions and communications
- Communications plan
- Alert and warning plan
- Personal emergency preparedness training for protective and medical actions for individuals to take before, during and after an ASHER event

Enhancements in communications, alert and warning plans:

The inclusion of personnel and facility preparedness through training, testing and improving of the four systems most often deployed as facility electronic security systems: video surveillance, perimeter and/or intrusion detection, electronic access control and building openings/door locking hardware systems.

Industry Impact: **High**

Supplemental Standards and Guidelines: Federal, State, Local Government and Industry Standards & Guidelines

- [“Security For Building Occupants And Assets,”](#) Whole Building Design Guide, National Institute of Building Sciences, 9/15/2017, web.
- [“PASS,”](#) SIA, web.
- [“State of School Safety Report 2018,”](#) Safe and Sound Schools, web.
- [“School Security Task Force \(reference documents\),”](#) New Jersey School Boards Association, web.
- [“What Makes Schools Safe?,”](#) New Jersey School Boards Association, web.
- [“Las Vegas After-Action Assessment: Lessons Learned from the Las Vegas Metropolitan Police Department’s Ambush Incident,”](#) U.S. Department Of Justice, Office Of Community Policing Services, web.
- [“MACTAC-NextGen Active Shooter Response,”](#) Ed Sanow, Hendon Publishing, web.
- [“Active Shooters Infographic,”](#) web.
- [“Active Shooter Recommendations and Analysis For Risk Mitigation,”](#) 2016 Edition As Released By The New York City Police Department, web.

Chapter 5 Risk Assessment

Reference: Section 5.4.2, Facility Risk Assessment (see also comments on Section 3.3.25: “Electronic Premises Security System”)

To be consistent with the terminology used in the security industry, “electronic premises security system” is usually four systems: video surveillance, perimeter and/or intrusion detection, electronic access control and a building openings/door locking hardware system.

Although it is a clarification in terminology, the importance of both facility practitioners and first responders being aware of individual electronic safety and security resources is high. A video surveillance system can provide improved situation awareness of where students or employees are exiting a building or taking refuge. A perimeter intrusion detection system can report unusual activity after hours. The electronic access control, together with door locking hardware, can maintain life safety through free egress while providing valuable functions like emergency lockdown, free egress or employee trace.

Reference: Section 5.4.2: “Availability of Building Map/Site Plan,” “Distance to and Capabilities of Medical Facilities:”

Consider the use of electronic maps and geographic information system (GIS) data featuring imagery, base maps, elevation, demographics, live feeds, landscape layers, nearby points of interest including hospitals, critical infrastructure and major transportation hubs. Apply same to each of the four aforementioned electronic security categories of video surveillance, perimeter and/or intrusion detection, electronic access control and building openings/door locking hardware system.

As stated, maps and demographic data, periodically updated, may be used as part of the risk assessment process. Building floor plans and campus plans may be used to display the real-time location of gunfire, explosion, glass breakage and aggressive behavior through the use of acoustic signature processing. Campus egress paths and door lockdown may be controlled in near real-time through the use of an electronic access control system and location map data.

Video surveillance, together with current map data, can verify camera views and provide visual verification of an incident in progress.

A real-time free space detection system using LIDAR sensors, together with current map data, can perform object recognition and deliver situation awareness of potential use cases experienced during an ASHER event:

- Movement and paths of crowd(s), students or employees outside campus buildings
- Illegal use of vehicles in pedestrian areas (recognition of vehicles and people in close proximity or on a projected path)
- Elevations of trees, objects and structures within the area detected by LIDAR sensors

Near real-time monitoring of keywords on social media feeds, with location of individuals through geofencing, mobile device location data and detection by wireless network.

Industry Impact: High

Supplemental Standards and Guidelines: Federal, State, Local Government and Industry Standards & Guidelines

(Also in *Section 4 Supplemental Standards*)

- [“What Makes Schools Safe?”](#) New Jersey School Boards Association, web.
- [“Las Vegas After-Action Assessment: Lessons Learned from the Las Vegas Metropolitan Police Department’s Ambush Incident,”](#) U.S. Department of Justice, Office of Community Policing Services, web.
- [“MACTAC⁸-NextGen Active Shooter Response,”](#) Ed Sanow, Hendon Publishing, web.
- [“Active Shooters Infographic,”](#) web.
- [“Active Shooter Recommendations and Analysis For Risk Mitigation,”](#) 2016 Edition As Released By The New York City Police Department, web.

8 [“Multi-Assault Counter Terrorism Training,”](#) FEMA, Brewer, ME Case Study, 1/8/2018, web.

Chapter 6 Planning/Coordination

Reference: 6.7.2. Guidelines and Procedures

For “Unified Tactical Considerations,” recommendation is to broaden to include the following:

(2) Unified Tactical Considerations

- a) Tactical Scenarios
- b) Tactical Solutions (stationary, existing on-site)
 - i. Electronic mass notification system with GIS mapping
 - ii. Accessible video surveillance live feeds and recordings
 - iii. Control of door opening/locking hardware/lockdown system
- c) Tactical Solutions (mobile)
 - i. Mobile command center or incident command vehicle
 - ii. Overwatch visible light, thermal imaging cameras and LIDAR
 - iii. Overwatch unmanned aerial system as above
 - iv. First-person view unmanned ground vehicle with video surveillance and chemical, biological, nuclear, radiological and/or explosive sensor array
- d) Tactical Solutions Operational Resources
- e) Tactical Solutions Training

For “interoperability among resources,” recommendation is to broaden to include the following:

(3) Interoperability among resources

- a) Communications interoperability
 - i. Between agencies
 - ii. Between first responder classes (law enforcement, fire, EMS, hazardous materials (HAZMAT), search and rescue, communications)
 - iii. To remotely control tactical solutions (stationary, existing on-site) from mobile command center or incident command vehicle

For “Social Media Management,” recommendation is to broaden to include the following:

(14) Social Media Management (See figure 2 and 3 on page 11)

- a) Preparation for Social Media Use
 - i. Assessment of social media resources and systems
 - ii. Prepare messaging
 - iii. Define roles
 - iv. Assign human social media response resources
 - v. Develop crisis-specific messages by scenario
- b) Social Media Crisis Operations and Engagement

- i. Communicating with the public regarding disaster preparedness
- ii. Communicating with the public during disaster response and recovery
- iii. Detect early warning messages
- iv. Community engagement activities
- v. Communicate with other organizations involved with disaster management
- vi. Monitor activity and messages by other organizations
- vii. Social media monitoring w/ geofencing of public safety announcements and public situation and sentiment
- viii. Leverage social media for post-disaster fundraising

Industry Impact: High

Supplemental Standards and Guidelines:

- “3 Tiers of a Social Media Crisis—and How to Manage Each One of Them,” PRNews, Jennings, 03/26/2018, Web.
- “Examining the Role of Social Media in Effective Crisis Management: The Effects of Crisis Origin, Information Form, and Source on Publics’ Crisis,” ResearchGate, Yan Jin et al, 10/17/2011, web.
- “3 Great Examples of Crisis Management on Social Media,” Fisher, 8/2/2013, web.
- “Six ways to start a social media crisis,” Fisher, 12/8/2015, web.

FIGURE 2 Crisis Management: Pre-social media engagement



FIGURE 3 Social Media Engagement



Chapter 7 Resource Management

Reference: NFPA 3000 7.1 – 7.4

No additional comments at this time.

Industry Impact: **Low**

Supplemental Standards and Guidelines:

- [“Active Shooter: How To Respond,”](#) DHS, Dec. 2, 2009, web.
- [“Active Shooter Response Plan Template,”](#) DHS, 2008, web.

Chapter 8 Incident Management

Reference: 8.1 – 8.8

Industry Impact: **Low**

Supplemental Standards and Guidelines:

- “Active Shooter Planning And Response: Learn How To Survive A Shooting Event In a Healthcare Setting,” Federal Bureau of Investigation, Healthcare & Public Health Sector Coordinating Council, International Association of Emergency Medical Services Chiefs (IAEMSC), 1/24/2017, web.
- “IS-100.LEB: Introduction to the Incident Command System (ICS 100) for Law Enforcement,” FEMA, web.
- “IS-100.LEB: Introduction to the ICS 100 for Law Enforcement, Sample Exam Answers,” FEMA Test Answers, web.

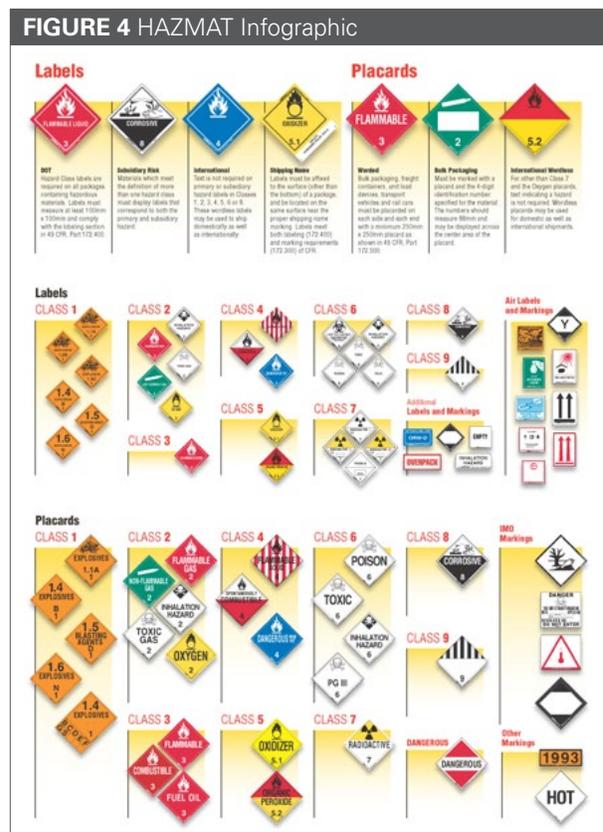
Reference: 8.4.2

Recommendation to list all relevant first responder categories, as the threat may be an active assailant (broader term) rather than an active shooter:

- Law enforcement
- Fire
- EMS
- HAZMATs include such substances as toxic chemicals, fuels, nuclear waste products and biological, chemical and radiological agents (see figure⁹)
- Search and rescue
- Communications

The International Association of Fire Chiefs restates and reaffirms its position in opposition to the consolidation of fire and emergency services departments with local law enforcement agencies, including the transition to public safety officers who are cross-trained to perform both fire/emergency medical services and law enforcement functions.

“Position: Consolidation of Fire/Emergency and Law Enforcement Departments and the Creation of Public Safety Officers,” web.



Credit: Labelmaster: HAZMAT Infographic: labels Placards and Markings Infographic: labels Placards and Markings

9 “HAZMAT Infographic: Labels, Placards and Markings,” Labelmaster, web.

Chapter 9 Facility Preparedness

Reference: 9.3.2 – 9.3.3

Recommendation to include standard response protocol (SRP), procedural documentation and signage as noted for business, pre-kindergarten (PK2), kindergarten - 12th grade (K12), community college (CC) categories (see links in Guidelines).

Recommendation to locate and identify all doors controlled and monitored for locking and door position status, by an automatic lockdown system. In such a system, the facility safety practitioner has the ability to initiate a “lockdown condition” for all doors equipped with electric locking devices and door hardware preventing free entry to the protected area functioning as an emergency shelter area during an ASHER event.

Additional recommendation for clear posting within the protected space of signage indicating door opening number or identification and location, procedure and sequence of operations during a manual or automated door lockdown scenario.

Recommendation to include reunification protocol as noted in guidelines below.

Industry Impact: High

Supplemental Standards and Guidelines:

Reunification

- http://iloveguys.org/srm_v2/SRM%20V2%20Single%20Pages.pdf
- http://iloveguys.org/srm_v2/SRM%20Parent%20Handout.pdf
- http://iloveguys.org/srm_v2/SRM%20V2%20Reunification%20Card.pdf
- http://iloveguys.org/srm_v2/SRM%20Signage.pdf

SRP K12

- <http://iloveguys.org/srp/SRP%20K12%20Operation%20Guidelines%202015.pdf>
- <http://iloveguys.org/srp/SRP%20K12%20Classroom%20Training%202015.pdf>

SRP PK2

- <http://iloveguys.org/srp/SRP%20PK-2%20Curriculum%20Workbook.pdf>

Lockdown Drill Guidance

- <http://iloveguys.org/srp/Lockdown%20Drill%20Guidance.pdf>

Teacher Guidance

- <http://iloveguys.org/srp/SRP%20K12%20Teacher%20Guidance.pdf>

SRP Business

- <http://iloveguys.org/srp/SRP%20BIZ%20Operation%20Guidelines.pdf>
- <http://iloveguys.org/srp/SRP%20BIZ%20Staff%20Handout%20v2.pdf>
- <http://iloveguys.org/srp/SRP%20BIZ%20Poster.pdf>

SRP CC

- <http://iloveguys.org/srp/SRP%20CC%20Trade%20and%20Tech%20Guidelines.pdf>

Student/Staff Handout

- <http://iloveguys.org/srp/SRP%20CC%20Student%20Staff%20Handout%20v2.pdf>

SRP Poster

- <http://iloveguys.org/srp/SRP%20CC%20Poster.pdf>

Medical Help Card

- <http://iloveguys.org/srp/SRP%20CC%20red%20green%20med%20card.pdf>

Reference: 9.4 Notification

See comments for the following:

- Reference: 17.3, warning, notification and crisis communications

Chapter 10 Financial Management

No additional comments at this time.

Chapter 11 Communications Center Support

Reference: NFPA 3000 11.6.2 Communications System Interoperability

First responder groups and agencies participating in the unified command shall incorporate periodic testing and demonstration of communications interoperability, including solution designers and solution providers as necessary. Communications system interoperability acceptance test criteria shall be developed, used and updated periodically.

First responder groups and agencies participating in the unified command shall incorporate potential public/private partnerships, as feasible, to use mobile broadband services as available as a backup to primary communications system.

First responder groups and agencies participating in the unified command shall consider the following potential technologies developed under DHS Science and Technology Directorate (S&T) Next Generation First Responder Apex Program (DHS-S&T APEX) as feasible, as available and as a backup to primary communications system: situational awareness systems, drones, datacasting and deployable communications¹⁰.

*Industry Impact: **High***

¹⁰ “DHS-S&T Integration Demonstrations,” web.

Chapter 12 Competencies for Law Enforcement Officers

No additional comments at this time.

Chapter 13 Competencies for Fire and EMS Responders

No additional comments at this time.

Chapter 14 PPE

No additional comments at this time.

Chapter 15 Training

Recommendation to include SRP, procedural documentation and signage as noted for business, PK2, K12 and CC categories (see links in Chapter 9 comments).

Chapter 16 Public Education

Supplemental Standards and Guidelines:

- [“Community Training: Surviving an Active Shooter Event,”](#) National Safety Council (NSC), web.
- [“Become an NSC Safety Ambassador,”](#) NSC, web.

Chapter 17 Public Information

Reference: 17.3, Warning, notification and crisis communications

This section provides general guidance for the inclusion of pre-scripted mass notification systems. An important point made is that organizations need to evaluate mass notification for individuals without access to mobile devices or “vulnerable” individuals, possibly interpreted as those individuals with disabilities or impairments recognized by The Americans with Disabilities Act (ADA).

The pre-scripted mass warning messaging is noted to have five basic requirements:

1. Who is sending the alert?
2. What is happening?
3. Who is affected?
4. What action should be taken?
5. What is the time and date stamp.

The ability to send important mass notifications or alerts to any number of people at once, allowing for immediate, individual responses with an audit trail is often a primary investment before other situation awareness tools. An “I’m OK” response plus the time of travel a mass notification alert took to reach an individual furthest from its origination is important. Notification of a moving threat to employees in proximity of the emergency is critical. Simply put, one-way communication is unacceptable in these cases.

Electronic Mass Notification Systems using mobile devices and digital signage

Reviewing and enhancing the basic requirements of a mass notification system, the practitioner may develop an enhanced list of requirements:

1. Who is sending the alert? *Enhanced requirement:* “Which verified agency, department or practitioner originated the alert”?
2. What is happening? *Enhanced requirement:* (could be several) Which of the publicly recognizable emergencies is expected to happen, is in progress or is confirmed to be concluded. Of course, the scope of an ASHER program is an active assailant, who could incorporate several threats below. A potential comprehensive list of potential emergencies follows:
 - a. Aggressive crowd or individual behavior*
 - b. Medical emergency
 - c. Fire emergency
 - d. Weather-related event
 - e. Flood
 - f. Release of hazardous substances, such as chemicals are released*
 - g. Vehicular threat (wrong way driver, vehicle used to endanger public: aircraft, train or vessel)*
 - h. Active assailant: threat of violence with lethal weapon(s); active shooter (with firearms)

- i. Explosions*
- j. Electrical grid malfunction or intentional damage
- k. Transportation structure failure (bridge, tunnel, freeway)
- l. Biological threat
- m. Nuclear substance threat
- n. Earthquake or volcanic eruption

*may also be under active assailant category

3. Who is affected? *Enhanced requirement:*
 - a. Push notifications to individuals, groups or community
 - b. Emergency notification via audible and visual signaling device with digital display messaging: ADA compliant, immediate and intrusive alerting, scripted visual digital display and verbal announcements, capability to alert people with visual or hearing impairments. Device complies with NFPA 72, Chapter 24, Layer One recommendation for immediate and intrusive alerting.
 - c. Change notification based on moving threat location to those in proximity of emergencies
 - d. Location of individuals through geofencing, mobile device location data, detection by wireless network
 - e. Response by student or employee of their status and location
4. What action should be taken?
5. Time and date stamp. *Enhanced requirement:* Location mapping through geofencing and mobile location-based services
6. *Enhanced requirement:* Mobile messaging latency or time from source notification initiation to receiving device alert process + time to receive message delivery receipt + time to receive recipient "new location" data.

Industry Impact: **High**

Supplemental Standards and Guidelines:

Although voice over IP (VoIP) and mobile messaging solutions are widely deployed, they rely on established standards in the information and communication technology infrastructure industry. To date, a standard providing the design and performance of mass notification systems originating from software-as-a-Service, VoIP or telephony systems, received by mobile devices or digital signage systems has not been developed.

SIA is currently considering development of such a standard: *"Standard for the design and performance of electronic mass notification systems using mobile devices and digital signage in an education facility."*

Chapter 18 Continuity of Operation

Reference: 18.2 Continuity

Recommendation to include guidance for the following criteria for continuity of electronic safety and security systems:

- Evaluation and selection of service and maintenance provider
- Periodic preventative maintenance and testing schedule
- Demand maintenance program supporting unforeseen outages
- Depreciation of electronic solutions and communications infrastructure; recommended upgrade cycle and budget development
- Value engineering and solution improvement process
- Periodic verification of electronic solutions and infrastructure for current and pending, relevant code compliance.
- Periodic re-evaluation and selection of service and maintenance provider

*Industry Impact: **Medium***

Chapter 19 Hospital Preparedness and Response for Out-of-Hospital ASHER Incidents

General note: *Because this section directly involves life safety and treatment, it should be referenced that this commentary, the standards and guidelines cited and the NFPA 3000 standard should not be considered substitutes for education in mass casualty incidents, or the NIMS and the ICS.*

Reference: 19.1.2 Purpose

Detailed guidance for health care triage and hospital incident command should reflect established SDO guidance for that discipline.

One example is the EMS “DISASTER” response mnemonic:

- D Detect
- I Incident Command
- S Scene Security and Safety
- A Assess Hazards
- S Support (determine need, order resources early)

*Industry Impact: **Medium***

Supplemental Standards and Guidelines:

Users of NFPA should also refer to the implementation of tasks described in the [Hospital Emergency Incident Command System \(HEICS\)](#)¹¹.

The authorities of San Mateo district medical emergencies service created the HEICS framework.

It consists in an algorithm of positions, the holders of which have a specific task in the event of an emergency situation. Each of these persons has his/her own listing of tasks to be carried out, so that he/she can guide the implementation of these tasks in the framework of an integral system if a disaster occurs. HEICS also includes listings of operations aimed at maximizing the overall efficiency, promoting the undertaking of responsibilities and facilitating the recording of key data. Several individuals can be available to cover a position assigned by the incident coordinator; in other cases, a single individual has to undertake more than one position, according to the listing of tasks.

The “*mass casualty management system*” is based on:

- Pre-established procedures to be used in daily emergency activities and adapted to meet demands of a major incident
- Maximizing usage of existing resources
- Multi-sector preparation and response
- Strong pre-planned and tested coordination
- This system is developed to accelerate and amplify daily procedures

¹¹ “[Planning and triage in the disaster scenario](#),” HEICS (Hospital Emergency Incident Command System), web.

- To maximize the use of the existing resources
- Establish a coordinated “multi-sector rescue chain”
- Promptly and efficiently bring disrupted emergency and health care services back to routine operations

The rescue chain, the essence of the mass casualty management system, involves the health department, private hospitals, police, fire department and nongovernmental organizations, transport services and communications. This chain starts at the disaster site (with activities such as initial assessment, command and control, search and rescue and field care), continues with transfer of victims to appropriate facilities (using procedures to regulate evacuation and ambulance traffic control), passes through hospital reception (with activation of the hospital disaster response plan) and ends only when the victims have received all emergency care needed to stabilize them.

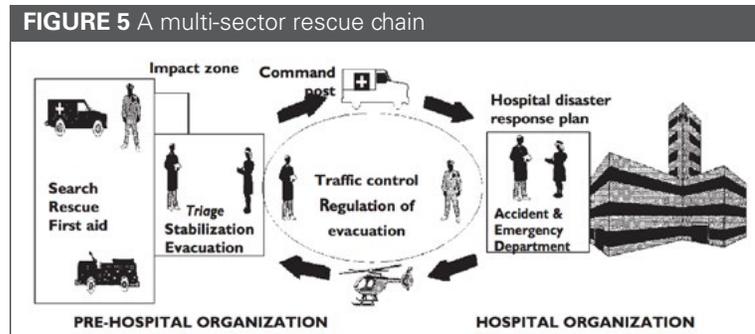


FIGURE 5 A multi-sector rescue chain
Credit: Establishing a Mass Casualty Management System, Washington, D.C. 1996

Reference: 19.2 Preparedness and Emergency Management

Regarding “spontaneous patient admissions,” and a dedicated hospital incident command, patient preparedness and distribution may be done differently in large cities. Where there is a mass casualty event, emphasis is placed on the time of treatment and severity of injuries and require transport time monitoring and hospital census (availability of care). This data may be accumulated and displayed at the EOC by a type of system known as a “digital sandbox.”

Industry Impact: **Medium**

Reference: 19.3 Patient Distribution

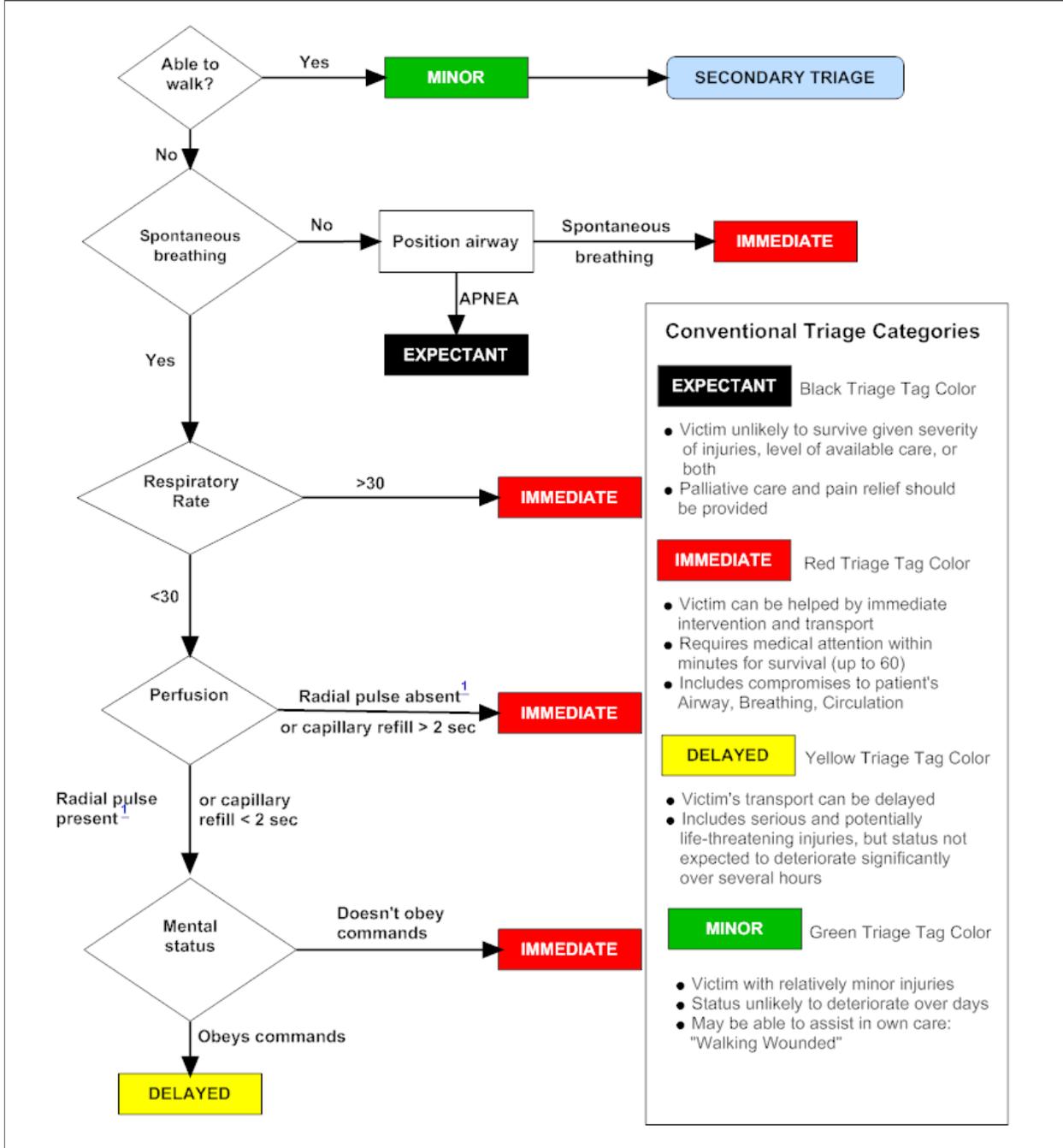
In NFPA 3000, the term “mass casualty incident plan” is used; other SDO in the EMS industries use both *mass casualty management system* and *multi-sector rescue chain* terms.

Industry Impact: **Medium**

Supplemental Standards and Guidelines:

- “Disaster Operating Guidelines Field Guide,” Eastern PA EMS Council, November 2017, web.
- “Fire And Rescue Departments of Northern Virginia Firefighting and Emergency Operations Manual, Multiple Casualty Incident Manual,” July 2017, web.
- “Three-Step Method for EMS Management of Bus Collisions,” Journal of Emergency Medical Services, Aug. 1, 2017, web.

FIGURE 6 Start adult triage



Credit: Radiology Emergency Medical Management, <http://www.remm.nlm.gov/StartAdultTriageAlgorithm.pdf>; adapted from original: Lou Romig, MD

Chapter 20 Recovery

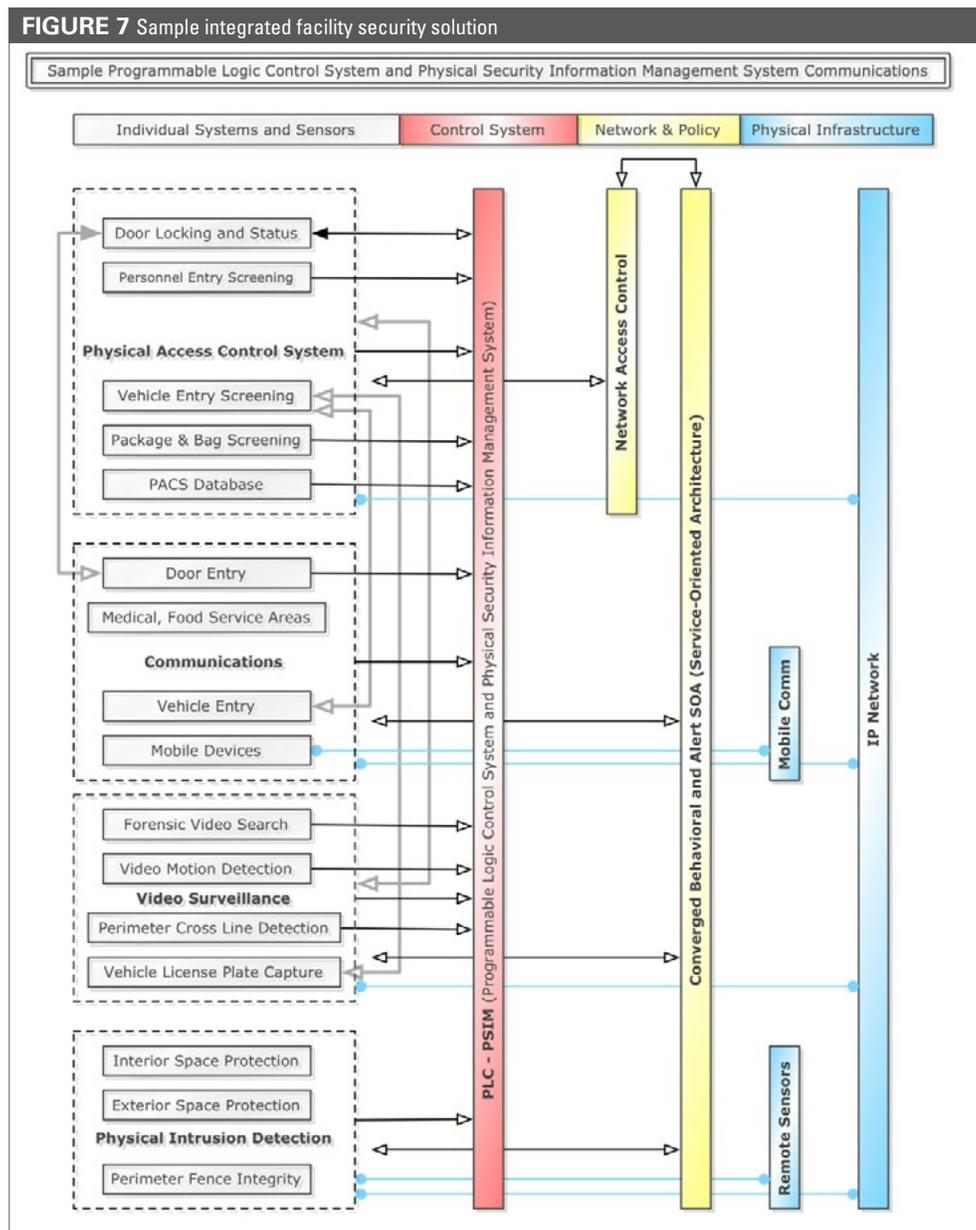
No additional comments at this time.

Annex A Explanatory Material

Reference: Annex A A.9.4.1

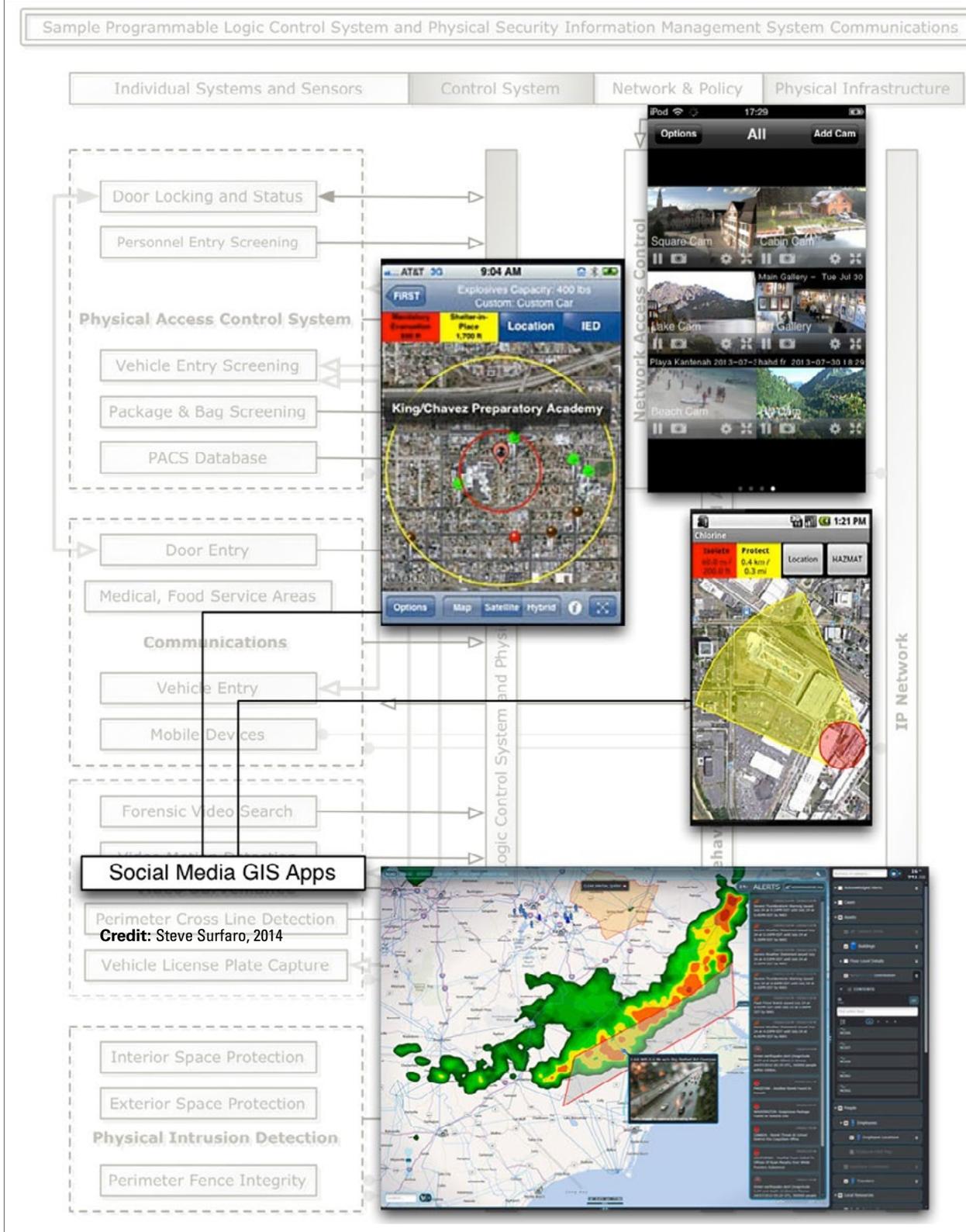
Recommendation to prioritize and widen the use of safety and security/surveillance and communications systems. Recommendation to prioritize “*Electronic Mass Notification Systems using mobile devices and digital signage*” described in Chapter 17 **as most critical system** for overall facility readiness improvement.

When considering improvement on other facility systems, it is recommended to consider a wider range of solution categories most appropriate for each facility’s unique use cases. The following diagrams represents potential opportunities for inclusion or improvement:



Credit: Steve Surfaro, 2014

FIGURE 8 Sample integrated facility security solution



Credit: Steve Surfaro, 2014

Annex B Laws, Regulations, Consensus Standards and Guidance Documents

No additional comments at this time.

Annex C Informational References

No additional comments at this time

Supplemental Standards and Guidelines:

- [“Resources for Active Shooter Incidents,”](#) Association of Public-Safety Communications Officials, web.
- [“Incident Command System Training,”](#) FEMA Emergency Management Institute, NIMS Training Program, ICS Resource Center, web.