



# RECOMMENDABLE

Commend Whitepaper on the New NFPA 3000 Standard



- 1. Changing times
- 2. The legal situation
- 3. Top protection priorities
- 4. Functionality and added value
- 5. A perfect service partner

## Communication that saves lives

### Why Incident Response Plans (IRP) are essential

Whether in companies, government agencies or public institutions – the need for reliable security technology is at a record high. Along with technology solutions, Commend fully supports ASHEPAR: **A**ctive **S**hooter **H**ostile **E**vent **P**reparedness **A**nd **R**esponse. Establishing action plans in life-critical situations helps protect vulnerable individuals and contain the threat when every second counts.

After the tragic fire at Our Lady of Angels, Chicago, Illinois, December 1, 1958 where 92 students and 3 teachers perished, fire safety and security in K-12's was forever changed. But has it really? There has not been a loss of life in a US K-12 from a fire since this date, but how many have perished from ASHE in the last 12 months?



# RECOMMENDABLE

Commend Whitepaper on the New NFPA 3000 Standard

## Guidance and assistance in accordance with NFPA 3000

### Changing times

We are living in a time that is characterized by insecurity. Extremism and terrorist threats have become regular topics in the news. Mass shootings and other attention-seeking acts of violence have left deep marks on the population. Many people are understandably concerned – and persons in

positions of responsibility are no exception. Managers, executives and security directors have ever increasing responsibilities that come with their roles as professionals. They are called upon to ensure the best possible protection of their staff during working hours. As a result, they are required to

take safety precautions in the interest of everyone within their scope of responsibility. This includes anyone from visitors in an office complex to customers in a shopping center to patients in a hospital. At the same time, barrier-free access has to be maintained in all relevant areas.

---

It is highly advisable to consult with a competent security provider early on so they can support and guide you through the planning process.

---

### Vague ideas


The applicable legal requirements for executives are getting more and more specific. Many US work protection laws, as well as NFPA 3000, will require employers to provide an individual written threat analysis for every area of activity within their company. This includes interviews with employees to determine their subjective awareness of risk scenarios. If it turns out that there are actual everyday situations where colleagues fear for their physical safety, the employer is mandated to take appropriate countermeasures. This is where things get tricky; what does “taking countermeasures” really mean?

In essence, many executives lack relevant know-how. Those with key responsibilities in less technical areas simply do not have the knowledge to translate identified security shortcomings into the equipment necessary to mitigate them. Even the best executive can feel overwhelmed when faced with questions such as, “*Do we need a new video surveillance system?*”, “*Should we get new fire alarms?*” or “*What about access control?*”. This is because, depending on the area of application, these issues may involve rather complex risk scenarios for a range of different target groups. Airports or railway

stations, for example, have a large number of employees working in different locations, in addition to being frequented by hundreds of passengers in multiple buildings. This often leads to rash decisions and grasping at every idea that promises to step up the current level of security. Be careful, if you approach the problem this way, you will run the risk of overreacting – using a sledgehammer to crack a nut, so to speak. **This is because taken in their context, threat situations and risk scenarios are highly individual, requiring a multiplicity of specific factors to be taken into consideration.**

## History of federal guidance

What guidance can we find from the federal government? The United States Department of Labor – Occupational Safety and Health Administration currently has no specific **OSHA** standards for workplace violence. However, under the **General Duty Clause**, Section 5(a)(1) of the Occupational Safety and Health Act of 1970, **employers are required to provide their employees with a place of employment that is “free from recognized hazards that are causing or are likely to cause death or serious harm.”** The courts have interpreted OSHA's general duty clause to mean that an employer has a legal obligation to provide a workplace free of conditions or activities that either the employer or industry recognizes as hazardous and that cause, or are likely to cause, death or serious physical harm to employees when there is a feasible method to abate the hazard. An employer that has experienced acts of workplace violence, or becomes aware of threats, intimidation, or other indicators showing that the potential for violence in the workplace exists, would be on notice of the risk of workplace violence and should implement a workplace violence prevention program combined with engineering controls, administrative controls, and training. Granted there may not be a specific OSHA standard for workplace violence. But the bottom line, under OSHA Directive Number: CPL 02-01-058 you can find Enforcement Procedures and Scheduling for Occupational Exposure to Workplace Violence under the General Duty Clause. Workplace Violence IS a recognized hazard!



---

Under the **General Duty Clause**, Section 5(a)(1) of the Occupational Safety and Health Act of 1970, employers are required to provide their employees with a place of employment that is “free from recognized hazards that are causing or are likely to cause death or serious harm.”

---

# RECOMMENDABLE

Commend Whitepaper on the New NFPA 3000 Standard

## How should you proceed?

### NFPA 3000 as a guideline

Governmental departments, official bodies and boards of trustees in many countries provide guidelines for business executives on how to handle work-related security issues. However, the main focus of these guidelines is usually on organizational issues and business processes. Technical aspects are usually treated only superficially and/or incompletely. For example, these documents typically provide general notes on resistance classes for doors and windows, or guidelines on intruder alarm

systems. However, crucial aspects such as fail-safe emergency communication are completely omitted. The same applies to standards that seek to improve security in residential and non-residential buildings. Where technology is concerned, their focus is exclusively on fire protection. NFPA 3000 provides clear guidelines for business executives on how to implement security measures and how to select the proper technical equipment. With its comprehensive set of rules, this standard

describes, for example, the technical systems suitable for calling help, triggering alarms, warning affected persons and transmitting instructions in individual security threat scenarios. NFPA 3000 also helps security managers to take all the measures that are required of them by law. Of course, the mere existence of a standard does not make its recommendations compulsory, but there are laws and directives that do.

“Let our advance worrying become advance thinking and planning.”

-Winston Churchill

### Baseline agency/department/organization protocols used for ASHEPAR

	FEMA Comprehensive Preparedness Guide (CPG) 101	Interagency Security Committee (ISC)	OSHA Guidelines for Preventing Workplace Violence	NFPA 3000
Common Elements	November 2010	November 2015	2016	December 2017
Risk Assessment	✓	✓	✓	✓
Preparedness	✓	✓	✓	✓
Unified Command	✓	✓	✓	✓
Integrated Response	✓	✓	✓	✓
Communication	✓	✓	✓	✓
Incident Response Plan	✓	✓	✓	✓
Training and Exercises	✓	✓	✓	✓
Evaluate Improvement	✓	✓	✓	✓



## Training and Exercise

One of the most important elements in fire safety is training and exercise. Every first grade student learns to expect a fire drill at least two times every school year. This continues through matriculation. But what can we do for ASHE training and exercises? There are many organizations and options to consider that provide guidance and training. Some programs focus on occupants while others focus on responders and building owners. Others on taking an active role in your own personal safety.

For example:

- Avoid - Deny - Defend from  
[Advanced Law Enforcement Rapid Response Training \(ALERRT\)™](#)
- Run - Hide - Fight  
[FEMA IS-907: Active Shooter: What You Can Do](#)
- ALICE:  
[Alert - Lockdown - Inform - Counter - Evacuate](#)

These are a few of the well known and highly accepted options for training and exercise. There are varying opinions on which training and exercises are the best approach. Some have even taken the

approach that it is too “scary” therefore do nothing to prepare. We should all be thankful for NFPA national standards with fire drill requirements. NFPA 3000 will be no different. Specific requirements for drills and exercise are coming for ASHE. **The question is, do we wait for the requirement/standard or do we begin the process now?**

$$\text{Risk} = \frac{\text{Threat} \times \text{Vulnerability} \times \text{Impact}}{\text{Countermeasures}}$$

If you understand the basic Risk formula, ask yourself these questions:

- *Do my electronic countermeasures increase or improve situational awareness during ASHE?*
- *Are we utilizing lasting and empowering technologies that improve operations and increase survivability?*
- *Have we trained and exercised our ASHEPAR utilizing our electronic countermeasures?*
- *Are our electronic countermeasures part of our EOP annexes?*

## The legal situation

What if we simply do nothing? Or are we led by a moral obligation to employees, students, constituents, visitors or customers to act? OSHA has made it abundantly clear you need to do something or face enforcement procedures that include fines. NFPA 3000 will soon advance by facilitating the code development for preparedness and response for ASHE.

How does this unfold? It works out more often today in the court of law. A personal injury lawyer for an employee may use some or all of the following legal terms: foreseeability which is a legal duty.

Without reasonable care, or what is also known as reasonable man test, there is the possibility of breach of duty. When best practice is not observed then proximate cause may be deemed by the court. Lastly if damage or injury occur, the action or even inaction may be defined as negligence.

**In the event of a scenario that involves personal damage, the official investigators will ask whether the person causing the injury should have reasonably foreseen the consequences that would**

**result because of his or her conduct.**

This is why many regional building regulations today require that building systems are to be constructed and maintained in such a way that public safety and law and order are not endangered. Applicable technical regulations intended to ensure these requirements are to be followed. Furthermore, each entrepreneur shall ensure that the building work complies with the accepted technical rules of engineering and required documentation.



**ADVANCED  
SECURITY  
COMMUNICATIONS**

# RECOMMENDABLE

Commend Whitepaper on the New NFPA 3000 Standard

## The proper solution for emergencies

### Finding appropriate technical equipment

According to the Interagency Security Committee (ISC), **“Those closest to the public address or other communications system, or who are otherwise able to alert others, should communicate the danger and necessary action.”** To avoid misunderstandings, it is important to remember that the new rules of application are intended only to ensure the best possible support of organizational processes for firms, government agencies and institutions. They do not provide any rules of conduct for specific incidents such as a mass shooting. This is because many firms and institutions have their own crisis management concepts. For this reason, the focus should rather be on implementing these individual concepts with the help of stable, fail-safe incident response plans (IRP). The challenge consists of finding an appropriate technical system whose solutions provide added value in crisis situations. **Technology is also the essential component of an effective implementation.** This includes the effective support

of the most essential crisis intervention routine: assessing situations and alerting security services or police forces.

**Multi-functional security communication systems are ideally suited for this purpose.** They are designed to support each item on the emergency and threat response agenda with latest-generation technology. Each system is different, as its composition depends on the assessment of the underlying technical risk management (see info box for details).

The key factor in deciding on technical equipment is security level as determined by way of a risk analysis.

→ Security Level 1 applies in low-risk environments with limited requirements.

→ Security Level 2 is recommended for environments involving a medium level of risk.

→ Security Level 3 is appropriate for potential high-risk areas.

The different system solutions all share the same basic structure:

The core element of a powerful **IRP** consists of an industrial-strength communications / intercom server as the system's communications hub. Connected to a (potentially unlimited) number of strategically positioned query point terminals and building alarm equipment, the server functions as an interface to all relevant security technology components, such as video surveillance or loudspeaker systems, digital mobile radios, and the telephone network. ISC also states, **“Internal communications with those in the immediate situation is critical. Security officials are encouraged to use any means necessary, including information technology platforms, software, or devices (e.g., computer messaging, mobile phone applications, etc.) to disseminate information to the workforce in a dynamic environment.”**



### 1| Alarm

- Who can trigger an alarm?
- Where are the **IRP** hotspots?
- Which emergency call terminals are available?



### 2| Verification

- Who verifies the alarm?
- What is the response procedure in case of an alarm?



### 3| Emergency Response

- How are security warnings communicated to affected persons?
- Which additional systems have to be controlled (e.g., CCTV, loudspeakers, access control...)?
- Will the appropriate security services be alerted?
- Which information will the security services require?
- How can the members of an internal crisis response team coordinate with each other?



# Top protection priorities



1

Alert helpers quickly!

2

Assess the situation!

3

Support crisis response teams!



Internal Control Center  
Crisis Response Team



Mobile Control Center  
DMR (Digital Mobile Radio)  
Smart Devices

Multi-functional  
Intercom solution



External Control Center  
Action Force



Public address systems  
Security levels 1 + 2 + 3



Touch-screen intercom systems for indoor use  
Security levels 2 + 3



Emergency call stations  
Security levels 2 + 3



Alarm button  
Security Level 1



## 4| De-escalation

- Will crisis intervention teams be given the required information and on-site directions?
- How will the on-site situation be determined?

## 5| Aftercare/Prevention

- Are action concepts being evaluated and developed further?

i

### Technical risk management:

The new NFPA 3000 standard calls for a technical risk manager to determine the required security level and for the solution to be implemented accordingly. This defines how the technical equipment will support the firm or institution in managing a dangerous situation or emergency.

It is therefore essential that concrete requirements and protection goals are defined right at the beginning of each planning stage. This allows for individual adjustments, as a primary school requires a different solution than a synagogue, for example.

**Deciding early on which functions are needed will help to keep the costs within the limits of what is technically necessary, and it will allow existing technical systems to be incorporated into new concepts.** Once the technical equipment has been selected, it has to be integrated into the organizational processes.

A risk manager will only have achieved his/her main objective when all crisis-specific processes have been improved.

# RECOMMENDABLE

Commend Whitepaper on the New NFPA 3000 Standard

## Functionality and added value in everyday situations

### Functionality in emergency situations

**A crucial factor is a bi-directional security communication system, i.e., one that provides direct voice communication connection between a caller and the appropriate control center. This is because an instant communication line via loudspeakers and microphones is essential for verifying and prioritizing alarms, and for coordinating appropriate countermeasures. Even if the person who triggered the alarm is unable to respond, the staff at the control center can still monitor the situation at the other end of the line acoustically over the microphone and take the necessary steps. Their response may involve anything from calling the police to establishing direct contact with a perpetrator over the intercom line. Moreover, this acoustic verification by control center staff also helps to prevent costly false alarms.**

#### IRP Hotspot 1

- Locations with a low risk potential
- Can be installed in many areas
- ADA/DDA compliant button
- Connect with speaker for 2-way communication

#### IRP Hotspot 2

- Locations with high risk potential
- Voice communication
- Activation of external cameras
- Confirmation
- Self-monitoring (24/7)
- ADA/DDA compliant button
- Ultimate availability
- Suitable for everyday use
- Vandal resistant

2

1

Alarm button with microphone

Emergency call point with video support



## Security and added value

**IRP** arrangements that are based on latest intercom technology have a unique advantage; they can be used efficiently for everyday communication tasks. **After all, it is for good reason that security specifiers consider systems as particularly useful if they can be used in an emergency as well as in everyday situations.** This is because experience shows that people must be fairly familiar with specific technical equipment before

they are sufficiently confident to use them in an emergency. One example is intercom systems in school classrooms, which can significantly improve regular day-to-day communication throughout the school and surrounding campus. **Systems like these can also be used for sounding the break signal, making announcements, providing information, coordinating security drills, or issuing situation-specific instructions.** A tailored intercom

system can also add significant value where internal communication at industrial plants and production facilities is concerned – e.g., improving communication between control stations and other work areas.

**Besides, operators are certain to benefit from a practical side effect: the systems' versatility and suitability for multiple purposes makes for a highly efficient investment** (think *indirect profitability / ROI*).



Smart indoor touch-screen terminal  
with integrated video camera

3

### IRP Hotspot 3

- Locations with high risk potential
- ADA/DDA compliant button
- Biometric reader
- Voice communication
- Integrated video communication
- Enhanced crisis communication
- Self-monitoring (24/7)
- Ultimate availability
- Modular and multi-functional, suitable for day-to-day use

# RECOMMENDABLE

Commend Whitepaper on the New NFPA 3000 Standard

## Beyond the usual standard

When it comes to quality,  
it's the details that count

Additional specifications in terms of equipment are imposed by external requirements on the hardware components – for example, if the devices are to be installed outdoors or indoors. The following example of a standard-compliant intercom station for indoor use illustrates some essential

key features: customers should verify that the devices are capable of **continuous self-monitoring to ensure their constant availability and functionality**. Another important feature is resistance against vandalism, attained through specially reinforced front panels. Polycarbonate is a

proven and reliable material for this kind of intercom station. An additional poke protection is also beneficial to have. The intercom station should also be designed to prevent the ingress of dirt or dust. Remember: the larger the call button the easier it'll be to operate in an emergency.





## A perfect partner

When implementing an emergency and threat response system service partners can be especially helpful, as they can guarantee products and services from a single source. **All security managers are therefore well advised to find a single-source solution provider – someone who can support and guide you from the concept phase through all stages of the planning process.**



Poke protection and special sabotage-proof screws

Vandalism-resistant high-grade steel surface, suitable for outdoor installation

Protected against ingress of moisture, dirt and dust

Two electret microphones for hands-free talking (max. speaking distance: 23 ft.)

Wide variety of housing stanchions available

An isolated building security platform is of little use – just like a dedicated evacuation solution that cannot be utilized for anything else. Instead you should select a provider who can supply the terminal devices as well as the server components, interfaces and easy-to-operate user surfaces. If your provider can also offer a high level of availability and quality, all the better. **Besides, you should ensure the availability of standardized interfaces to third-party systems so you can integrate your existing components into your new system.** Ideally, your offer should include a visualization feature to enable you to custom-configure central components such as control desks to suit your user needs. Please note: innovative service providers will already offer you the option of integrating mobile subscriber units into the network via emergency applications. In this age of mobile devices, a feature like this will improve your system's security communication capabilities by several degrees.

# RECOMMENDABLE

Commend Whitepaper on the New NFPA 3000 Standard



COMMEND

## 7 Hints for security managers

1. Find a single-source solution provider.
2. Consult with your provider early on so they can support and guide you through the planning process.
3. Make sure they can also offer you a high level of availability and quality of their solutions.
4. Focus on solutions that include the terminal devices as well as the required server components, interfaces and easy-to-use user surfaces.
5. Ensure the availability of standardized interfaces to third-party systems so you can integrate your new system with your existing components.
6. Verify that the solution includes a visualization feature that enables you to custom-configure central components such as control desks to suit your user needs.
7. Request the ability to integrate mobile subscriber units into the network via emergency applications. In this age of mobile devices, a feature like that will improve your system's security communication capabilities by several magnitudes.

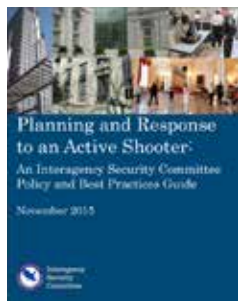
i

Contact our Regional Managers, all of whom are FEMA ICS 100 and active shooter trained, to learn more about technical risk management and the advantages and possibilities of an emergency and threat response system.

Contributors:  
Brad Anderson  
Commend Inc.  
[b.anderson@commendUSA.com](mailto:b.anderson@commendUSA.com)

Jerry Wilkins, PSP®  
Active Risk Survival  
[jerry@activerisksurvival.com](mailto:jerry@activerisksurvival.com)

## Preparedness Response Resources



## Head Office in US

Commend Inc.  
63 Ramapo Valley Rd. Suite 201  
Mahwah, NJ 07430  
Tel.: +1-201-529-2425  
E-mail: [sales@commendusa.com](mailto:sales@commendusa.com)

**ALICE**  
TRAINING INSTITUTE

Alert  
Lockdown  
Inform  
Secure  
Escalate

**Active Risk Survival**  
Tactically Aware, Technically Competent