NFPA 730 & 731

New premises security system standards strive to make the world a safer place

• by Jim Lardear

There is a bumper sticker that says, "Lead, follow, or get out of the way." Obviously, if you are reading it, you are following the car ahead. But for how long depends on things you can control, like your driving style, and things you cannot control, like traffic conditions. The discussion and debate surrounding the NFPA's efforts to essentially fill a void and develop installation and maintenance standards and guidelines for premises security systems has a little of this feeling about it.

Video surveillance systems have long been a part of many companies' security programs. Simple and effective, they not only deter crimes but help solve them.

While the NFPA's development of codes is an open, consensus-based process, its attempts to form a comprehensive set of guidelines and standards for premises security is leading the industry to a destination it has been unable to reach on its own, namely regulation. As a result, there is some sentiment in the security industry that the NFPA, which is primarily known for fire prevention, electrical, and life safety codes, should instead get out of its way.

"Companies don't mind being regulated, as long as they are in compliance," says R. T. Leicht, SFPE, Chief Fire Protection Specialist, Office of the Delaware State Fire Marshal. "But they don't want the requirements to be too rigid, or find themselves forced into doing things they were not ready for or prepared to do."

The reality is that the NFPA is not overstepping its bounds by developing security standards for public access buildings. The two new documents currently being developed – **NFPA 730:** *Guide for Premises Security* and **NFPA 731:** *Installation of Premises Security Equipment* – will join the NFPA's 300 other safety codes and standards that already influence practically every building and process in the United States.

C. Fannin, III, President and CEO of SafePlace Corp. (Wilmington, Del.). Fannin also serves as a member of the NFPA's Premises Security Committee.

According to Fannin, the lessons learned from the tragedy of that day, the resulting demand for enhanced security for people in public access facilities, and the reality of the continued complacency with regard to the security of private-sector facilities, confirmed the need for the development of NFPA's premises security documents.

"Studies confirm that most Americans consider security and safety among their top concerns when selecting public access facilities like hotels, academic institutions, and hospitals," he says. "As a result, businesses and institutions must demonstrate a commitment to personal safety and security – evidence that they are striving for a higher standard of care."

The NFPA's code-development process focuses on building a true consensus by encouraging the broadest possible participation by interested members across industries. It acts as an independent third party, advocating scientifically-based consensus codes and standards developed by more than 6,000 volunteers who are not required to be NFPA members

"Studies confirm that most Americans consider security and safety among their top concerns when selecting public access facilities like hotels, academic institutions and hospitals."

A Need for Leadership

"Our world has changed since 9/11. Personal safety is now everyone's concern; where they work, when traveling, on college campuses, when attending public functions, and anytime they are away from home," says John

PICTUREQUEST

A security guard swipes a coded ID card through a magnetic card reader to gain access to a secure area.

Work on NFPA 730 and NFPA 731 included representatives from the insurance industry, American Society for Industrial Security (ASIS), Security Industry Association (SIA), Central Station Alarm Association, American Hotel and Lodging Association, Virginia Crime Prevention Bureau, International Council of Shopping Centers, Underwriters Laboratories, International Fraternal Police Association, and manufacturers of security products, among others.

In fact, according to Richard P. Bielen, PE, chief systems and application engineer for the NFPA and staff liaison for both standards, ASIS submitted 53 proposals out of 297 on NFPA 730 and 25 proposals out of 73 on NFPA 731.

On Again, Off Again

In July 1994, after numerous requests by the insurance industry, the NFPA Standards Council voted to establish a Burglary/Security Alarm Systems Project. At the direction of the NFPA Board of Directors, the Council reconsidered the project and solicited input from the security industry in the early summer of 1995. However, by July 1995, the Standards Council voted not to proceed with the establishment of standards for the applications and installation of burglary/security systems due to a lack of widespread interest in moving forward.

"However, later that year, the insurance industry re-initiated their request on the broader subject of premises security that led to a panel discussion at the November 1995 NFPA Fall Meeting in Chicago," explains Wayne D. Moore, PE, Hughes Associates Inc. (Warwick, RI) and Chair of the NFPA 730 and & 731 project. "Again in January 1996, the NFPA Standards Council voted not to proceed on a premises security project because they did not perceive a clear consensus on the issues surrounding the project."

According to Moore, three years later in June 1999, the insurance industry asked the Council to reconsider the project and in November 1999 the NFPA Board of Directors decided to move ahead with a full set of codes for the built environment including a new Premises Security Project.

In April 2000, the Standards Council re-affirmed the decision to proceed with the premises security project and by July 2000 it had approved the initial scope of the project.

In January of 2001 the Council revised the scope, which now reads:

> *"The Committee shall have the primary responsibility for documents on the overall security program for the protection of premises, people, property and information specific to a particular occupancy. The Technical Committee shall have responsibility for the installation of premises security systems."*

According to Bielen, the "on again, off again" history of the project was due to opposition from outside organizations and the NFPA's internal concerns about doing something beyond the normal scope of the *National Electrical Code (NEC)* and the *National Fire Codes*. It finally began in earnest in 2000.

CORBIS

The Standards Council appointed the start-up roster for the Technical Committee on Premises Security in April 2001.

"The Technical Committee initially wanted to develop an installation document but the NFPA Standards Council directed them to publish a premises security document first, or concurrently, with an installation standard," Bielen says. "The committee decided to develop two new documents: a premises security document (NFPA 730) and an installation document (NFPA 731)."

Separate task groups were formed to develop each proposed document; both were then reviewed and modified by the Technical Committee.

NFPA 730 and NFPA 731

In a nutshell, NFPA 730 is the "what," while NFPA 731 is the "how" of premises security.

NFPA 730, *Guide for Premises Security,* describes construction, protection, occupancy features, and practices intended to reduce security vulnerabilities to life and property. It covers a security vulnerability assessment, designing a security plan, interior protection, exterior protection, security guards, special events, and security measures for occupancies.

NFPA 731, *Standard for the Installation of Electronic Premises Security Systems,* covers the application, location, installation, performance, testing, and maintenance of physical security systems and their components.

If the development processes continue on schedule, both NFPA 730 and 731 are scheduled to be voted on by the NFPA membership in June 2005, with standards being issued as soon as July.

One of the differences in the development processes for NFPA 730 and NFPA 731 is that the former is a "guide," while the latter is a "standard."

According to the NFPA, a "guide" is a document that is advisory or informative in nature and that contains only non-mandatory provisions. Although a guide may contain mandatory statements, such as when it can be used, the document as a whole is not suitable for adoption into law.

"The NFPA 730 occupancy-based application document proved to be the most difficult to gain consensus on among the committee membership," Moore says. "Originally begun as a code, the document transformed to a recommended practice and finally became a guide; NFPA 730 is now a Guide for Premises Security."

By definition, an NFPA standard is a document that contains only mandatory provisions using the word "shall" to indicate requirements, and which is in a form generally suitable for mandatory reference by another standard or code, or for adoption into law. Non-mandatory provisions are located in an appendix or annex, footnote, or fine-print note and are not to be considered a part of the requirements of a standard.

The "authority having jurisdiction" – or AHJ – can be an organization, office, or individual responsible for enforcing the requirements of a code or standard, or for approving equipment, materials, an installation, or a procedure.

One concern of security professionals is that even though a guideline is not enforceable, it may open the Pandora's box of liability. Already, premises security lawsuits are among the fastest growing segments of personal injury lawsuits. Some estimates place the average award for verdicts and settlements as being in excess of $1.2 million.

NFPA 730

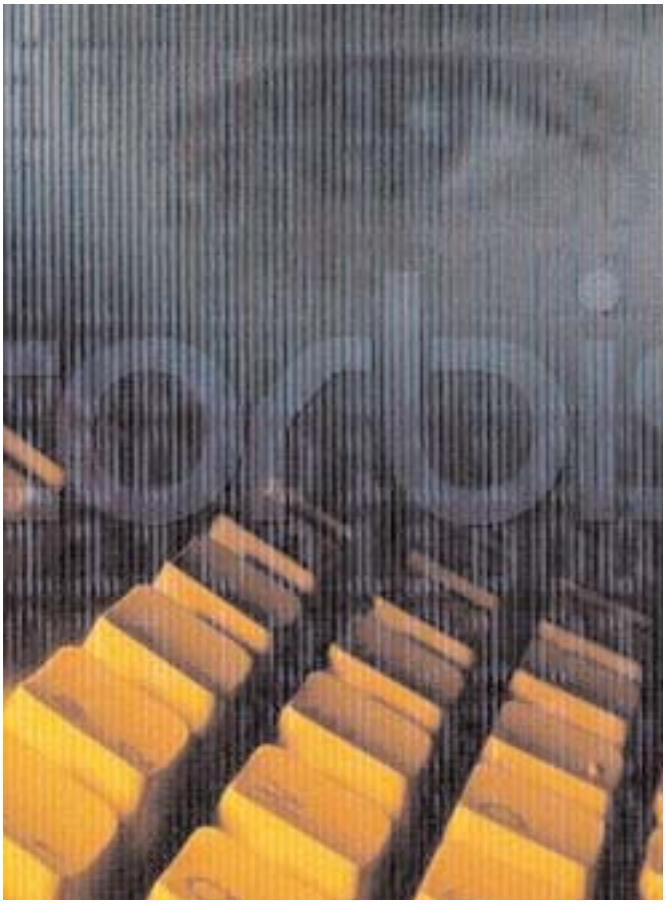
According to NFPA's Bielen, NFPA 730 covers the recommended exterior and interior security features for different types of occupancies, from one- and two-family dwellings to industrial complexes. The first half of NFPA 730 is devoted to the basic details of interior and exterior security devices and systems and the roles and responsibilities of security personnel.

"It goes far beyond electronic security systems by covering matters such as a security vulnerability assessment, designing a security plan, interior protection, exterior protection, duties of security guards, special events, and security measures for occupancies," Bielen says. "Access control is also highlighted as a feature found in most occupancies."

The developers of NFPA 730 recognized that not all public access facilities have identical security vulnerabilities, as a result, there is no single set of "one size fits all" security countermeasures. "However, groups of like facilities (hotels, academic institutions, health care facilities, etc), do experience many common security issues," notes Safeplace's Fannin.

"Discussion of these common issues and examples of effective countermeasure techniques, as are provided in NFPA 730 through a 'tool-box' approach, can provide

In a nutshell, NFPA 730 is the "what" while NFPA 731 is the "how" of premises security.



Computer and IT systems are now just one element a company needs to evaluate in conducting an overall security vulnerability assessment.

valuable assistance to facility security planners when combined with a proven risk assessment methodology – the security vulnerability assessment," Fannin says.

Bielen agrees. "NFPA 730 stresses conducting a security vulnerability assessment (SVA) and the details of designing a security plan," he says.

As outlined by NFPA 730 Chapter 5.2, the seven-step SVA is a powerful technique that complements and builds upon existing security, safety, and risk management processes, with the overall objective of mitigating potential adversarial events.

Fannin recommends that in the course of conducting an SVA, all existing site security features – "current layers of protection" (including both site security features and safety measures) – be evaluated objectively and comprehensively.

"The reality of private sector security has changed a great deal," Fannin notes. "Present day private sector security issues are more complex and diversified than traditional security practice areas, not the least of which include computer and IT security, workplace violence, and the threat of domestic terrorism," Fannin says. "In these complicated times, security professionals must begin with an SVA."

The next 11 chapters of NFPA 730 provide recommendations specific to certain types of occupancies including shopping centers, restaurants, office and apartment buildings, one- and two-family dwellings, and educational, industrial, lodging, healthcare and parking facilities.

NFPA 731

NFPA 731, which provides specifications for installing electronic security systems and devices in the included types of facilities, is being developed as a standard and is similar to NFPA 72, *National Fire Alarm Code*.

"The NFPA Standards Council correctly recognized the differences between fire alarm and security issues, establishing separate and distinct technical committees for each," SafePlace's Fannin says. "Appropriately, NFPA 730 and 731 do not regard fire alarm systems."

"For the first time in the history of security systems there is proposed a standard with its primary purpose 'to define the means of signal initiation, transmission, notification and annunciation as well as the levels of performance and reliability of electronic security systems,'" Moore says.

"Present day private sector security issues are more complex... including computer and IT security, workplace violence, and the threat of domestic terrorism."

The scope of NFPA 731 also includes wiring requirements, power supplies, supervision, testing and maintenance, access control, and surveillance.

According to Moore, the primary focus for the first edition of NFPA 731 will be on intrusion detection systems and the reduction of false alarms. "NFPA 731 addresses Access Control, CCTV and the integration of these systems as well as the interface of premises security systems with the life safety systems," he says.

Moore notes that NFPA 731 is not designed to require a level of premises security; rather it establishes the minimum required levels of performance, extent of redundancy, and quality of installations. It also does not establish the only methods by which the requirements are to be achieved.

"The requirements of NFPA 731 are designed to increase the quality and reliability of installations and reduce the inordinate number of false alarms due to poor

CORBIS

installation, application, and training," Moore says.

Proposed requirements of NFPA 731 include: "Premises security system plans shall be developed by persons who are experienced in the proper design, application, installation, and testing of premises security systems. The system designer shall be identified on the system design documents. Evidence of qualifications shall be provided when requested by the authority having jurisdiction. Examples of qualified personnel shall include, but not be limited to, the following:

(1) Equipment manufacturer trained and certified personnel.

(2) Personnel licensed and certified by state or local authority.

(**3**) Personnel certified by an accreditation program acceptable to the AHJ."

Other requirements that differ from NFPA 72, Moore points out, include: "Signals from exterior detection devices shall not be retransmitted to the authority having jurisdiction unless physical verification of an intrusion is made." Physical verification is required to be made either on-site or by video.

The NFPA 731 technical committee decided that for the first edition, NFPA 731 will only address the protected premises from the property line to the interior of the premises and that it will not address the operation of the Central Station as it relates to security signal monitoring.

"The committee was aware of other documents that affected the installation of security systems and has referenced or incorporated the requirements of applicable UL, SIA and other industry standards," Moore notes.

Role of NFPA 70

While the *National Electrical Code*, NFPA 70, has always had requirements for the installation of premises security systems, Moore says many installers ignored them because the law enforcement community was not aware of the code requirements.

While NFPA 730 has very little to do with the *National Electrical Code (NEC)*, NFPA 731 references it for wiring and emergency power supply requirements. "NFPA 731 features the power supply requirements (primary and secondary), wiring complying with NFPA 70 and testing and maintenance requirements," Bielen says.

NFPA 731 specifically requires that "The installation of all wiring, cable, and equipment shall be performed in a workman like manner in accordance with NFPA 70, *National Electrical Code*, and specifically with Articles 725 or 800, where applicable. Optical fiber cables shall be protected against mechanical injury in accordance with Article 770."

Conclusion

While both premises security documents make their way through the remaining cycles of public review to an anticipated vote in June, the debate over the NFPA's leadership role in developing meaningful practices for security features in public access buildings will continue to rage.

PICTUREQUEST

One of the areas covered by NFPA 731 is closed circuit TV (CCTV) and video surveillance systems.

"Ultimately, if [security and real estate interest groups] are required to comply with the guidelines and standards, NFPA 730 and NFPA 731 should level the playing field for all premises security system installers and designers as they will all be working off the same document with the same requirements," Bielen says. "It should also improve installation quality and reduce false alarms."

As Moore points out, while most police departments currently have little or no input to security systems design, application and installation, they are certainly affected by the industry's quality of workmanship or lack thereof.

"These departments, in response to their frustration of numerous false alarms from poorly installed or misapplied security systems, have begun the implementation of local ordinances to fine the owners, and in some cases the monitoring companies, when a system has reached a predetermined level of false alarms," Moore says. "In some extreme cases the police are refusing to respond to a premises security alarm signal when the system has cried wolf too many times in a week or month."

In Moore's opinion, the development and implementation of NFPA 730 and 731 will help to reduce the false alarms and give the law enforcement community more confidence in installed security systems.