Overview of NFPA 730 and 731, NFPA's New Security Standards

by Raymond A. Grill, P.E.

Over the last three plus years, a newly formed technical committee of the National Fire Protection Association (NFPA) has developed two new technical documents dealing with security in the built environment. This new technical committee is called the Technical Committee on Premises Security and they have prepared NFPA 730, *Guide for Premises Security* and NFPA 731, *Standard for the Installation of Electronic Security Systems.*
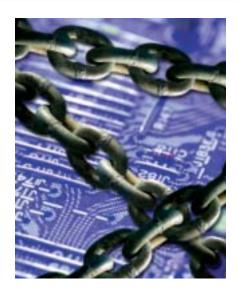
These documents will be presented to the membership of NFPA for approval at its annual meeting June 6-10, 2005, held in Las Vegas, Nevada.

The Process

This project was first started by NFPA in 1994 at the request of interested members of the association. The project was cancelled, and then restarted in 2000 when the NFPA Standards Council approved a scope for the Premises Security project.

The scope of the Technical Committee on Premises Security states: "This 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 Committee shall have responsibility for the installation of premises security systems."

Raymond A. Grill is president of Sako & Associates, Inc, a national security consulting firm. He also serves as the secretary of the NFPA Technical Committee on Premises Security. This is his first article for **Facilities Manager.** *He can be reached at rgrill@rjagroup.com.*

NFPA's standards development procedure is a consensus process that allows any interested party to participate. These documents have been available for public review and comment since August 2003.

Standards versus Guides

The development of security standards by NFPA has been controversial. There had been a strong contingent of end users who initially expressed strong concern over the development of security standards, particularly in light of the litigious nature of our society. The main concern was trying to develop a "one size fits all" standard that may not take into consideration the multitude of factors that are required to be incorporated in the development of a security plan for a facility.

From the onset, the committee was in reasonable agreement that the document providing criteria for design and installation of electronic security systems (NFPA 731) should be a standard. The committee had numerous debates on what type of document NFPA 730 would become. Ultimately, the committee wrote NFPA 730 as a guide.

NFPA 731, *Standard for the Installation of Electronic Security Systems*, is written to be referenced by other documents. Reference documents could include bid specifications and contract documents.

NFPA 730, *Guide for Premises Security,* is informative in nature and, does not include any mandatory requirements.

NFPA 730, Guide for Premises Security

The scope of the *Guide for Premises Security* is broad in nature and will allow for inclusion of new information and guidance in many areas of security for future revisions. The guide describes features and practices that can be implemented in buildings to reduce security vulnerabilities.

Chapters 1 through 4 provide basic information on the document, including the scope, purpose, and application statements. The overall goal of the guide is to provide a framework for assessing the security needs of a facility and to provide guidance for implementing a security program to address those needs.

Chapter 5 provides a seven-step process for developing a vulnerability assessment that is the cornerstone for a security plan.

Chapter 6 provides a comprehensive review of perimeter security measures. These measures include fences and other physical barriers, protective lighting, ironwork (e.g., bars and grills), glazing materials, passive barriers, and electronic security devices.

Chapter 7 describes the usage of and provides guidance for the application of various types of common physical security devices including builders hardware, locks, doors, windows, safes, vaults, and strong rooms.

Chapter 8 provides guidance in the development of interior security measures to protect specific areas or information. This chapter also reviews the different types of systems and equipment that can be deployed as security measures.

Chapter 9 discusses guidance in the application of security personnel and provides direction in this area. Security personnel can be an effective and necessary component of a security program.

Chapter 10 provides guidance on the development of a security plan and recommends features that should be included.

Chapters 11 through 22 provide direction in the development of security plans for specific occupancies and lists unique issues that should be considered in developing those plans.

Colleges & Universities

Chapter 11 provides guidance regarding security for educational facilities including colleges and universities. It reviews the history of the *Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (Jeanne Clery Act)*, a federal law that requires colleges and universities to disclose certain timely and annual information about campus crime and security policies, and provides the basic requirements of this Act.

This chapter discusses the goal of a campus security program and elements of the program necessary to meet the goal and the *Jeanne Clery Act*. The elements of the program are identified and each element is discussed. They include:
1. Record keeping system
2. Communication system
3. Training program
4. Campus law enforcement
5. Security surveys
6. Access control system
7. Security for campus housing
8. Security for research facilities
9. Security equipment

The scope of the Technical Committee on Premises Security states: "This 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. . ."

NFPA 731, Standard for the Installation of Electronic Security Systems

As discussed earlier, NFPA 731 is written as a standard and is intended to be referenced by other documents such as bid specifications and local jurisdictions or building codes. The scope of NFPA 731 covers the application, installation, performance, testing, and maintenance of physical security systems and their components.

The purpose of the standard is to define the means of signal initiation, transmission, notification, and annunciation as well as to establish levels of performance and reliability of electronic security systems. The standard also establishes minimum levels of performance, quality of installation, and where redundancy is required.

Looking into the Future

NFPA 730 provides a tool for systematic security program development. NFPA 731 provides a baseline for quality electronic security system design and installation. As end users, engineers, and manufacturers become more aware of these documents, it is expected that they will eventually become the foundation for development of security plans in the built environment. ⚱