(3) Tools required for the professional installation of raceways
(4) Restrictions of raceways

A.7.7.2 Underground/direct burial, pole-to-pole outside/UV protected, and return air plenum/plenum rated are examples of different insulation jacketing.

A.7.7.4 It should be the responsibility of the installer to use the appropriate connectors and methods of installation as dictated by the equipment and cable manufacturers' instructions. The selection of connectors should be based on a consideration of the environment, the conductor type, and the specific use (control, power, video, or data).

A.7.7.5 The applications for wiring within video surveillance systems are as follows:

(1) Control
(2) Power
(3) Video signal transmission

Because sufficient voltage and signal levels are imperative for proper system operation, consideration should be given to designing voltage drop (power and signal) allowances that would result in adequate operating voltage (or signal) at the various pieces of equipment.

A.7.7.5.1 The purpose of low-voltage control cabling is to carry various low-voltage signals to devices within the video surveillance system. Such devices can include, but are not limited to, the following:

(1) Remote positioning devices (pan/tilt units, scanner units, domes)
(2) Cameras (primary input power)
(3) Zoom lenses
(4) Auxiliary devices (low-voltage wipers and washers, low-voltage heaters and blowers, remote relays)

A.8.1.2.5 To minimize the unintentional operation of a portable device, factors such as jarring, contact with clothing, and similar sources should be considered.

A.8.2.2.8 The party responsible for the protected premises should ensure that this training takes place. In addition, employees should be trained to follow the procedures provided by their employer and the law enforcement agency having jurisdiction.

Δ **A.8.2.2.9** Off-premises locations that are used to receive holdup alarm signals should be equipped to retransmit signals to the law enforcement center that serves the property. Alarms are usually annunciated at a monitoring station. One example of off-premises locations that can receive alarm signals is one that complies with UL 827, *Standard for Central-Station Alarm Services*.

A.8.3.2.5 The intent of a duress system is to notify on-site personnel of a potentially hostile civil disturbance or emergency at the protected property and for summoning assistance to the area of the civil disturbance or emergency.

A.8.4.2.1 To reduce the incidence of inadvertent ambush signals, the following steps should be taken:

(1) If an ambush feature is provided in a control unit that is also used to operate other systems, the default setting should be that it is disabled.
(2) An ambush signal should be sent only by a unique code.
(3) A control panel that is also used to operate other systems should not derive the ambush code from an existing operating code such as a "user code plus ambush digit" sequence.

A.8.4.2.4 Each person who is expected to use an ambush alarm initiating device should be instructed to follow the procedures provided by the operator of the protected premises and the law enforcement agency having jurisdiction.

Δ **A.8.4.2.5** Alarms are usually annunciated at a monitoring station. One example of off-premises locations that can receive alarm signals is one that complies with UL 827, *Standard for Central-Station Alarm Services*.

A.9.2.1 These signals can include, but are not be limited to, the following:

(1) Alarms (including intrusion detection, holdup, and duress)
(2) Supervisory
(3) Trouble
(4) Restorals
(5) Open/close events
(6) Access control activity
(7) Video surveillance
(8) Audio surveillance

A.9.3.1 This section does not include any requirements for the handling or dispatching of calls for assistance and should be directed only at electronically received signals.

A.9.3.4.4 The determination of the type of detection device to be used should be based on an SVA for the facility. NFPA 730 can be used.

Building designers should consider security through environmental design and should provide zones immediately around the facility to ensure security of the grounds and the safety of the personnel within.

A.9.3.5.1 Standby power should have sufficient capacity to be able to operate HVAC necessary to maintain the environmental range of the monitoring equipment. Lighting should be provided to allow operators to perform normal functions.

A.9.3.5.1.1 The emergency power supply system (EPSS) can be used to supply other building loads. The EPSS should be sized to handle all loads simultaneously without having to shift other loads off the system. When life safety equipment is connected to the EPSS, consideration should be given to increasing the EPSS to level 1, type 10.

Δ **A.9.3.5.1.4** Guidance on preventing unauthorized access to the power supply can be found in UL 827, *Standard for Central-Station Alarm Services*.

A.9.3.6.3 All training should be in compliance with the manufacturer's recommendations, and a program should be in place for the continuing education of operators. Resources for this education include, but are not limited to, the Central Station Alarm Association, the Security Industry Association, and the Association of Public Communication Officers.

A.9.3.9.2.1 The list should contain, at a minimum, a contact name, phone number, after-hours cell phone number, and service contract information for each provider.

A.9.3.9.3.2 At a minimum, equipment should be able to operate within an environment of high-energy radio frequencies. In

addition, the equipment should not interfere with or be interfered with by any electronic equipment within the facility. The equipment should also be shielded from electromagnetic interference and radio frequencies as required.

A.9.3.9.4 Special consideration and contingency plans need to be considered. If the monitoring station is receiving signals from any high-risk facilities as defined by the Department of Homeland Security (DHS), provisions should be considered for implementing emergency transfer to the backup location.

A.9.6.1.1(4) Cross-zoning is one method of MTV. This method is used where there are technology limitations with the installation environment. An analysis of the application and use of cross-zoning should be performed, because this method might not be appropriate in many locations. With this method, at least two sensors within the same area of coverage should be installed. In this case, all sensors within the area should have tripped before an alarm is generated. The use of cross-zoning for intrusion detection systems is not the same as cross-zoning for fire alarm systems.

It is intended that cross-zoning would use separate sensors, not two detection means within a single sensor. This is a method of "dual technology." Cross-zoning is best achieved by using two separate sensors. Both could use the same technology or different technologies, which could include the use of a door contact for one of the zones.

A.9.6.1.1.1.2 The intent of 9.6.1.1.1.2 is for the monitoring station to call the protected premises first to verify the signal. It is realized, however, that there could be cases in which the protected premises might not have phone service. In those cases, the monitoring station can make the first call to a primary contact number that is provided by the system user.

A.9.6.1.1.2 Remote video verification (RVV) is intended to be used as a supplement to enhanced call verification (ECV). If through the use of RVV it is apparent that a crime or unauthorized entry is taking place at the protected premises, the information obtained can be transmitted or communicated to the public safety agency so it can coordinate the response protocol.

A.9.6.1.1.3 Remote audio verification (RAV) is intended to be used as a supplement to ECV. If through the use of RAV it is apparent that a crime or unauthorized entry is taking place at the protected premises, the information obtained can be transmitted or communicated to the public safety agency so that it can coordinate the response protocol.

RAV can be one way or two way. With one-way RAV, the monitoring station can listen in to the protected premises after an alarm activation. With two-way RAV, the monitoring station can, in addition to listening in, engage in a conversation with individuals who are on the protected premises.

A.9.6.3.1 The term *immediately* in this context is intended to mean "without unreasonable delay." Routine handling should take a maximum of 90 seconds from receipt of the alarm signal by the monitoring station until the initiation of notification to the public safety agency.

A.9.6.4.2.1 The term *immediately* in this context is intended to mean "without unreasonable delay." Routine handling should take a maximum of 90 seconds from receipt of the alarm signal by the monitoring station until the initiation of notification to the public safety agency.

A.9.6.5.1 The term *immediately* in this context is intended to mean "without unreasonable delay." Routine handling should take a maximum of 90 seconds from receipt of the alarm signal by the monitoring station until the initiation of notification to the public safety agency.

A.9.6.6 Facility hazards information should be provided to the first responders and can include information on rapid entry systems, dangerous chemicals or gases, explosive materials, or any other dangerous condition that might exist. Information on special security notices such as attack dogs, smoke bandits, chemical releasing agents, or security traps should also be maintained.

A.9.7.2 Transmission methods are changing. The uses of traditional landline-based communication methods are no longer as common as they once were. Voice over Internet Protocol (VoIP), facility and non-facility based as provided by common carriers, cable communication providers, and Internet providers, is becoming the new norm. The users of these communication methods need to be aware that control units that use communication technologies that are based on the public switched telephone network (PSTN) and using plain old telephone service (POTS) might not function on these new communication paths. Having a test signal sent in once every 7 days adds a level of reliability to verify that there is an active communication path between the protected premises and the monitoring station.

A.9.7.6.1(4) The intent of 9.7.6.1(4) is not to limit each line to 3000 transmitters but to require that if 3000 transmitters are exceeded on a single path, a redundant path is provided. This is to be considered primarily when broadband communication (Internet) solutions are used.

A.9.7.6.2 An inventory of spare equipment at the monitoring station allows personnel to replace any failed piece of equipment.

A.9.7.7.1(3) The intent of 9.7.7.1(3) is not to limit each line to 3000 transmitters but to require that if 3000 transmitters are exceeded on a single path, a redundant path is provided. This is to be considered primarily when broadband communication (Internet) solutions are used.

A.9.8 These records include, but are not limited to, the following:

(1) Signal history
(2) Documentation of personal identification codes (PICs)
(3) Public safety agency notification information

Note: Although the information on the PICs should be retained, it should be kept confidential and made available on a need-to-know basis.

A.10.1 More stringent inspection, testing, and maintenance procedures that are required by other parties can be permitted.

A.10.1.2 Equipment performance can be affected by building modifications, occupancy changes, changes in environmental conditions, device location, physical obstructions, device orientation, physical damage, improper installation, degree of cleanliness, or other obvious problems that might not be indicated through electrical supervision.

Δ **A.10.1.3** The premises security system provider responsible for the premises security system is the individual or organization

that ensures that inspection, testing, and maintenance are performed.

A.10.2.1 Examples of system defects and malfunctions are a trouble signal to the control panel or controller, a reader that is not operating, a video surveillance camera that is no longer providing an image, and other similar events.

A.10.2.1.1 The time period to initiate a repair should be less than 24 hours based on an agreement with the owner and the premises security system provider.

A.10.2.1.2 Notification to the owner is so that other security measures can be implemented.

A.10.2.2 Temporary mitigating measures should be considered by the owner or responsible party during impairments based on an SVA to the protected property or the occupants. Depending on the SVA, the AHJ can be consulted. The recommendations from the consultation should be implemented for the period that the system is impaired.

A.10.2.5 Additional security measures might be needed during the period of the impairment. These impairments can be caused by, but are not limited to, the following:

(1) Telecommunication errors
(2) Accident
(3) Fire
(4) Acts of God
(5) Loss of carrier
(6) Other transmission method failures

A.10.3.4.1 Door assemblies that are incorporated into the premises security system need to be periodically inspected to ensure they function correctly. Mechanical components and subcomponents (e.g., door leaves, hinges, locks, door closers) can prevent the door assembly from being able to perform its security function if they are malfunctioning, broken, or missing.

A.10.3.4.2(1) The factory training and certification should be specific and current to the equipment that is being used, and proof of this factory training and certification should be made available to the AHJ upon request.

A.10.3.5.1 In addition to advising the personnel within the protected premises that the system is being tested, repaired, or maintained and that signals generated from the system(s) should not be acted upon, the owner or responsible party should be advised that the system or a part of the system might not be fully functional during the testing, repairing, or maintenance procedure and that appropriate safeguards should be taken, based upon the perceived risk.

The party responsible for the protected premises should also be informed that if the system is placed into a degraded mode, some, if not all, information from those nodes can be lost during the time in which the node(s) is down.

A.10.4.2.2 This section requires that only the portions of the system that might have been affected by a modification need to be tested. As an example, if a door contact is added to zone 12, then only zone 12 is required to be tested. If there is a change to several zones, then only those zones would be required to be tested.

On the other hand, if there is a change to the system firmware or software that could affect the entire system, then the entire system should be tested.

A.10.5 Premises security systems and other systems and equipment that are associated with security systems and accessory equipment should be tested at the frequencies according to Table A.10.5.

Table A.10.5 Test Frequency

System, Device, or Equipment	Frequency
Intrusion detection system	Annually
(1) Exterior detectors	Annually
(2) Interior detectors	Annually
Holdup, duress, or ambush system	Annually
(1) Portable devices	Annually
(2) Exterior fixed devices	Annually
(3) Interior fixed devices	Annually
Access control system	Annually
(1) Readers	Annually
(2) Position switches	Annually
(3) Electric hardware	Annually
(4) Request-to-exit devices	Annually
CCTV system	Annually
(1) Camera enclosures	Annually and before adverse weather conditions
(2) Recorders	Annually
Sounding devices	Annually
Batteries — general tests	Annually
Off-premises transmission equipment	Quarterly or by automatic monthly test
Interface equipment	Annually

N **A.10.6.1** Equipment should be covered under a service agreement. Any device or system not functioning as designed should be repaired or replaced on a priority basis. The priority basis should be established by procedures developed in the SVA, manufacturer's instructions, or by the applicable standards.

Δ **A.11.2** Typical standards include UL 60950-1, *Standard for Information Technology Equipment – Safety – Part 1: General Requirements*; FCC 47 CFR Part 15; "Radio Frequency Devices"; and UL 1037, *Antitheft Alarms and Devices*.

Annex B Camera Specifications

This annex is not a part of the requirements of this NFPA document but is included for informational purposes only.

B.1 Cameras. For cameras placed to record images at a point of customer transactions, such as a teller window, the area of interest (face, license plate, etc.) should cover a minimum of 15 percent of the camera's field of view under normal resolution of 300 horizontal lines (HL) or more. Action within the scene requires that at least 20 percent or more of the overall width of the scene be used. For an average human head that is 15.24 cm (6 in.) wide, a 0.914 m (3 ft) wide field of view meets this guideline. For a license plate width of approximately 304.8 mm (12 in.), a 1.828 m (6 ft) field of view is sufficient.

The focal length necessary to achieve an approximately 0.914 m (3 ft) wide field of view for a given detector size and camera-to-subject distance is provided in Table B.1(a) (SI Units) and Table B.1(b) (U.S. equivalent units). The camera has to be in focus at the position of this subject.

Table B.1(a) and Table B.1(b) are based on the following calculations using either the scene width formula or the scene height formula.

[B.1a]

$$f = c\left(\frac{d}{w}\right)$$

or

[B.1b]

$$f = v\left(\frac{d}{h}\right)$$

where:
f = focal length of lens
c = width of the charge-coupled-device (CCD) chip
d = distance from camera
w = width of field of view
v = height of CCD chip
h = height of field of view

Cameras that provide overviews of interior and exterior locations should have their focal lengths selected to meet the field-of-view requirements of the AHJ. Note, however, that exit cameras should have sufficient depth of field to be in focus at distances of 0.914 m (3 ft) and beyond to ensure that subjects exiting are in focus.

Another method takes into account the total viewing area of the scene as a percentage of the monitor. Calculate the viewing area of the scene and also of the critical viewing area by multiplying the horizontal and vertical dimensions *[see Table B.1(c)]*. Divide the critical viewing area by the total viewing area to get the size of the critical viewing area in the monitor.

If the proportion of the critical viewing area is as expected, use the calculated focal length. If not, then change the focal length until the correct proportion is found, or change the distance of the camera until the correct proportion is found. If this does not solve the problem, a new lens might have to be chosen that is nearer to the requirement.

Table B.1(b) Approximate Focal Length Needed for 3 ft Wide Field of View

Detector Size (in.)	Focal Length Based on Distance to Subject					
	2 ft	5 ft	10 ft	15 ft	20 ft	30 ft
¼	2.3	5.9	11.7	17.6	23.5	35.2
⅓	3.1	7.8	15.7	23.5	31.3	47.0
½	4	10.1	20.2	30.3	40.4	60.7

Table B.1(c) Field of View

Camera Formats (in.)	Horizontal (mm)	Vertical (mm)
¼	3.2	2.4
⅓	4.4	3.3
½	6.4	4.8
⅔	8.8	6.6

B.2 Example. A 8.46 mm (⅓ in.) camera is viewing an entrance gate to a factory. The car coming through the gate is the critical view.

⅓ chip

Width (c) = 4.8 mm = 0.048 m (0.15 ft)

Height (v) = 3.6 mm = 0.036 m (0.11 ft)

Distance to gate (d) = 30.48 m (100 ft)

Width of gate (w) = 3.65 m (12 ft)

Car dimension (front) = 1.524 m × 1.524 m (5 ft × 5 ft)

Focal length $f = c \times (d/w)$ = 0.048 m × (30.48 m/3.65 m) = 0.40 m [0.16 ft × (100 ft/12 ft) = 1.33 ft]

Scene height $h = v \times (d/f)$ = 0.036 m × (30.48 m/0.4 m) = 2.75 m [0.11 ft × (100 ft/1.33 ft) = 9 ft]

Scene area = 3.65 m × 2.74 m = 10 m^2 (12 ft × 9 ft = 108 ft^2)

Critical area = 1.524 m × 1.524 m = 2.3 m^2 (5 ft × 5 ft = 25 ft^2)

Percent size of car in monitor = 25 × (100/108) = 23.1 percent

The car covers about 23 percent of the monitor. This allows positive identification of the car coming through the gate.

Table B.1(a) Approximate Focal Length Needed for 0.914 m Wide Field of View

Detector Size (m)	Focal Length Based on Distance to Subject					
	0.6096 m	1.524 m	3.048 m	4.572 m	6.096 m	9.144 m
0.0762	2.370104	1.79832	3.56616	5.36448	7.1628	10.72896
0.100584	0.94488	2.3744	4.78536	7.1628	9.54024	14.3256
0.1524	1.2192	3.07848	6.15696	9.23544	12.31392	18.50136

Scene identification should require that each camera within a system is able to be differentiated by its image's physical appearance. No system should have any two cameras looking from the same angle down two identical hallways. Each scene should be separable by visual recognition. The installer should follow the manufacturer's recommendations concerning the various compatibility issues that occur between the cameras and lens. Such compatibility issues can be physical or electronic.

B.3 Megapixel (MP) Cameras. The megapixel size for MP cameras should be based on the field of view and necessary needs for the ability to zoom in on a fixed image.

Annex C Camera Selection

This annex is not a part of the requirements of this NFPA document but is included for informational purposes only.

C.1 Criteria. A number of common camera selection criteria should be reviewed by the system installer prior to the installation to verify that the design objective is met. The criteria are as follows:

(1) Monochrome or color
(2) Light level and sensitivity
(3) Resolution
(4) Backfocus adjustment
(5) Format
(6) Sync and phase

C.1.1 Monochrome or Color. All white balance settings on or within the camera are set according to the manufacturer's specification to provide proper color rendition. In the event of a dual-chip technology camera system, the installer should perform setup procedures deemed necessary by the manufacturer to provide a proper white balance during high-light situations and proper black/white (B/W) sensitivity during low-light situations.

C.1.2 Light Level and Sensitivity. Sensitivity, measured in footcandles or lux (lumens per square meter), indicates the minimum light level required to get an acceptable video picture. Sensitivity at faceplate indicates the minimum light required at the charge-coupled-device (CCD) chip to get an acceptable video picture. Minimum scene illumination indicates the minimum light required at the scene to get an acceptable video picture.

To see properly, a video surveillance camera requires a certain amount of light produced by natural or artificial illumination. B/W cameras work with any type of light source, but color cameras need light that contains all the colors in the visible spectrum.

The amount of light is defined by lux or footcandles. One lux is a candlelight volume at a 0.914 m (3 ft) distance. The following are some examples of natural light:

(1) Full daylight is 10,000 lux (929 footcandles).
(2) Very dark day is 100 lux (9.3 footcandles).
(3) Twilight is 10 lux (0.93 footcandles).
(4) Deep twilight is 1 lux (0.093 footcandles).
(5) Full moon is 0.1 lux (0.0093 footcandles).
(6) Quarter moon is 0.01 lux (0.00093 footcandles).

A good B/W camera can see in full-moon conditions. However, a color camera might need additional illumination in low-light conditions.

Usually light falls on the subject. A certain percentage is absorbed and the balance is reflected. The reflected light moves toward the lens in the camera. Depending on the iris opening of the camera, a certain portion of the light falls on the CCD chip. This light then generates a charge, which is converted into a voltage. The following variables should be listed on the data sheet to indicate the minimum scene illumination:

(1) Reflectance
(2) F-stop
(3) Usable video
(4) Automatic gain control (AGC)
(5) Shutter speed

C.1.2.1 Reflectance. Light from a light source falls on the subject. Depending on the surface reflectivity, a certain portion of the light is reflected back toward the camera. Following are a few examples of surface reflectivity:

(1) Snow is 90 percent.
(2) Grass is 40 percent.
(3) Brick is 25 percent.
(4) Black is 5 percent.

Most camera manufacturers use an 89 percent or 75 percent (white surface) reflectance surface to define the minimum scene illumination. If the actual scene has the same reflectance as in the data sheet, then there is no problem, but in most cases this is not true. A black car will reflect only 5 percent of the light, so at least 15 times more light is required at the scene to give the 75 percent reflectance.

C.1.2.2 Lens Speed. The reflected light starts moving toward the camera. The first device it meets is the lens, which has a certain iris opening. While specifying the minimum scene illumination, the data sheet usually specifies an F-stop of F1.4 or F1.2. The F-stop gives an indication of the iris opening of the lens. The larger the F-stop value, the smaller the iris opening, and vice versa. If the lens being used at the scene does not have the same iris opening, then the light required at the scene needs to be compensated for the mismatch in the iris opening.

C.1.2.3 Usable Video. After passing through the lens, the light reaches the CCD chip and generates a charge that is proportional to the light falling on a pixel. This charge is read out and converted into a video signal. Usable video is the minimum video signal specified in the camera data sheet to generate an acceptable picture on the monitor. It is usually measured as a percentage of the full video.

C.1.2.4 AGC. As the light level reduces, the AGC switches on and the video signal gets a boost. Unfortunately, the noise present also gets a boost. However, when the light levels are high, the AGC switches off automatically, because the boost could overload the pixels, causing vertical streaking and so forth.

The data sheet should indicate if the AGC is on or off when the minimum scene illumination is being measured. If the data sheet indicates AGC is "on," but in reality the AGC is "off," then the minimum scene illumination in the data sheet should be modified.

C.1.2.5 Shutter Speed. Most cameras now have an electronic shutter speed that allows the user to adjust the timing of the charge read of the CCD chip. The standard readout is 50 times [phase alternate by line (PAL)] and 60 times [National Television Standards Committee (NTSC)] per second. If the shutter

speed is increased to 1000 times per second, for example, the light required at the scene should be 20 times more (for PAL). Increasing the shutter speed allows the picture to be crisper but requires more light.

C.1.3 Resolution.

C.1.3.1 All cabling and signal transmission methods should be installed with the proper connections, splices, and amplification to ensure that the image resolution is maintained at the maximum capability of the system's design.

C.1.3.2 IP camera resolution is measured in native and enhanced resolution scales. IP cameras will generally have a native resolution that can be digitally enhanced for higher resolution.

C.1.4 Backfocus Adjustment. The term *backfocus* refers to the course adjustment on the camera that positions the imager behind the lens. This adjustment allows for the proper positioning of the fine-focus adjustment on the lens. *Focus* refers to adjustment of the distance between the lens and the imager device in the camera. Focusing aligns the focal plane of the lens with the imager in the camera. When focusing, the iris of the lens must be opened to create the shortest depth of field. The lens should be focused and then the iris closed to increase the depth of field. An installer must know the relationship between F-stop and depth of field and how to properly focus both manual and auto-iris lenses.

C.1.5 Format. Knowing the size of the imager is necessary in selecting the appropriate focal lens to provide the desired view.

C.1.6 Sync and Phase. Power requirements of the video equipment are determined and established during the design phase. The line-locking feature of a camera means that the camera's vertical sync pulse locks to the incoming alternating current (ac) power line frequency. The reason is to ensure that the vertical pulses from many different cameras occur at the same time, eliminating any vertical roll when the cameras are switched. Direct current (dc)–operated cameras cannot be line-locked. Vertical sync of each camera should be adjusted according to the manufacturer's instructions.

C.1.7

C.1.7.1 Frame Rate. Most IP cameras have the ability to select how many frames per second a camera will send digital video. A frame is an individual picture that is taken. Standard movie-quality video is 30 frames per second, however the human eye can only register the difference in frames per second in motion video when the frames per second is 15 or lower. An increase of frames per second will increase video clarity and storage requirements, and a decrease in frames per second will decrease video clarity and storage requirements.

C.1.7.2 Compression. Compression is an algorithm that takes certain frames, called key frames, and measures them against other frames of video after the key frame. The differences between the key frames and the frames after the key frame are the only data sent for each frame.

C.1.7.3 Bandwidth. Bandwidth is the amount of data, measured in bytes, that the digital video will require on the network in order to transmit the video.

C.1.7.4 Bandwidth Calculators. Bandwidth calculators are tools provided by the camera and NVR manufacturers that approximate the bandwidth required for an IP video surveillance system.

N Annex D Homeland Security Advisory System

This annex is not a part of the requirements of this NFPA document but is included for informational purposes only.

N **D.1 General.** A recommended threat response elevation system was originally developed by the United States Department of Homeland Security (DHS). As threat conditions rise, it is recommended that facilities implement an appropriate corresponding set of protective measures to further reduce vulnerability and increase response capability. [**730:**B.1]

The following threat response recommendations are voluntary. [**730:**B.1]

N **D.2 Threat Conditions and Associated Protective Measures.** There is always a threat of a terrorist attack. Each threat condition assigns a recommended level of alert appropriate to the increasing risk of terrorist attacks. Threat conditions contain suggested protective measures that the government and the public can take, recognizing that the heads of federal departments and agencies are responsible for developing and implementing appropriate agency-specific protective measures. [**730:**B.2]

N **D.2.1 Normal Condition.** A normal condition is when there is a low risk of terrorist attacks. The private sector should consider the following protective measures:

(1) Refine and exercise prearranged protective measures.
(2) Ensure that personnel receive proper training on the Homeland Security Advisory System and specific prearranged department or agency protective measures.
(3) Institute a process to ensure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks and that all reasonable measures are taken to mitigate these vulnerabilities. Homeowners and the general public can develop a household disaster plan and assemble a disaster supply kit.
(4) Check communications with designated emergency response or command locations.
(5) Review and update emergency response procedures.
(6) Provide the public with any information that would strengthen its ability to act appropriately.

[**730:**B.2.1]

Homeowners and the general public, in addition to the actions taken for the low threat condition, should take the following steps:

(1) Update their disaster supply kits.
(2) Review their household disaster plans.
(3) Hold household meetings to discuss what members would do and how they would communicate in the event of an incident.
(4) Develop more detailed household communications plans.
(5) If they are apartment residents, discuss with building managers steps to be taken during an emergency.
(6) If they have special needs, discuss their emergency plans with friends, family, or employers.
(7) Increase surveillance of critical locations.
(8) Coordinate emergency plans with nearby jurisdictions as appropriate.

(9) Assess whether the precise characteristics of the threat require the further refinement of prearranged protective measures.
(10) Implement, as appropriate, contingency and emergency response plans.
[**730:**B.2.1]

Homeowners and the general public, in addition to the actions taken for the normal threat conditions, should take the following steps:

(1) Be observant of any suspicious activity and report it to authorities
(2) Contact neighbors to discuss their plans and needs
(3) Check with school officials to determine their plans for an emergency and procedures to reunite children with parents and caregivers
(4) Update household communications plans
[**730:**B.2.1]

N **D.2.2 Elevated Condition.** An elevated condition is declared when there is a credible threat risk. In addition to the measures taken in the previous threat conditions, the private sector should consider the following protective measures:

(1) Coordinate necessary security efforts with federal, state, and local law enforcement agencies, the National Guard, or other security and armed forces.
(2) Take additional precautions at public events, possibly considering alternative venues or even cancellation.
(3) Prepare to execute contingency procedures, such as moving to an alternative site or dispersing the workforce.
(4) Restrict access to a threatened facility to essential personnel only.
[**730:**B.2.2]

Homeowners and the general public, in addition to the actions taken for the normal threat conditions, should take the following steps:

(1) Review preparedness measures (including evacuation and sheltering) for potential terrorist actions, including chemical, biological, and radiological attacks.
(2) Avoid high-profile or symbolic locations.
(3) Exercise caution when traveling.
[**730:**B.2.2]

N **D.2.3 Imminent Condition.** An imminent condition reflects a credible, specific, and imminent threat risk. Under most circumstances, the protective measures for an imminent condition are not intended to be sustained for substantial periods of time. In addition to the protective measures in normal and elevated threat conditions, the private sector should consider the following general measures:

(1) Increase or redirect personnel to address critical emergency needs.
(2) Assign emergency response personnel and pre-position and mobilize specially trained teams or resources.
(3) Monitor, redirect, or constrain transportation systems.
(4) Close public and government facilities not critical for continuity of essential operations, especially public safety.
[**730:**B.2.3]

Homeowners and the general public, in addition to the actions taken for the previous threat conditions, should take the following steps:

(1) Avoid public gathering places such as sports arenas, holiday gatherings, or other high-risk locations.
(2) Follow official instructions about restrictions to normal activities.
(3) Contact employers to determine status of work.
(4) Listen to the radio and TV for possible advisories or warnings.
(5) Prepare to take protective actions such as sheltering-in-place or evacuation if instructed to do so by public officials.
[**730:**B.2.3]

N **D.3 Preparing for Terrorism.** Wherever they are, individuals should be aware of their surroundings. The very nature of terrorism suggests there might be little or no warning. [**730:**B.3]

N **D.3.1** Individuals should take the following steps:

(1) Take precautions when traveling.
(2) Be aware of conspicuous or unusual behavior.
(3) Do not accept packages from strangers.
(4) Do not leave luggage unattended.
(5) Promptly report to police or security personnel unusual behavior, suspicious packages, and strange devices.
(6) Do not be afraid to move or leave if you feel uncomfortable or if something does not seem right.
(7) Learn where emergency exits are located in buildings you frequent. Notice where exits are when you enter unfamiliar buildings. Plan how to get out of a building, subway, or congested public area or traffic. Note where staircases are located. Notice heavy or breakable objects that could move, fall, or break in an explosion.
(8) Assemble a disaster supply kit at home and learn first aid. Separate the supplies to take if evacuation is necessary, and put them in a backpack or container, ready to go.
(9) Be familiar with different types of fire extinguishers and how to locate and use them. Know the location and availability of hard hats in buildings in which you spend a lot of time.
[**730:**B.3.1]

N **D.3.2** Private sector facilities should take the following steps:

(1) Consider all the precautions prescribed for individuals.
(2) Develop written policies and procedures for terrorist events, train all personnel to them, and test their effectiveness.
(3) Provide a prepared on-site area of refuge for guests and employees should an off-site consequence prevent travel from the facility. Preparations should include provision of nonperishable food and drinking water, battery-powered commercial radio or television, first aid supplies, sanitation supplies, flashlights, and so forth.
[**730:**B.3.2]

N **D.4 Protection Against Cyber Attacks.** Cyber attacks target computer or telecommunication networks of critical infrastructures such as power systems, traffic control systems, or financial systems. Cyber attacks target information technologies (IT) in three different ways. The first type of attack is a direct attack against an information system through the wires alone (hacking). The second type of attack takes the form of a physical assault against a critical IT element. The third type of attack

originates from the inside as a result of a trusted party with access to the system compromising information. [**730:**B.4]

Both individuals and private sector facilities should be prepared for the following situations:

(1) To be without services that people normally depend on and that could be disrupted — electricity, telephone service, natural gas, gasoline pumps, cash registers, ATM machines, and Internet transactions
(2) To respond to official instructions (such as general evacuation, evacuation to shelter, or shelter-in-place) if a cyber attack triggers other hazards, for example, hazardous materials releases, nuclear power plant incident, dam or flood control system failures

[**730:**B.4]

N **D.5 Preparing for a Building Explosion.** Explosions can collapse buildings and cause fires. Both individuals and private sector facilities can do the following:

(1) Regularly review and practice emergency evacuation procedures.
(2) Know where emergency exits are located.
(3) Keep fire extinguishers in proper working order. Know where they are located and learn how to use them.
(4) Learn first aid.

[**730:**B.5]

Additionally, private sector facilities should keep the following items in a designated place on each floor of the building:

(1) Portable, battery-operated radio and extra batteries
(2) Several flashlights and extra batteries
(3) First aid kit and manual
(4) Several hard hats
(5) Fluorescent tape to rope off dangerous areas

[**730:**B.5]

N **D.6 Bomb Threats.** If a bomb threat is received, get as much information from the caller as possible. Keep the caller on the line and record everything that is said. Then notify the police and facility security. [**730:**B.6]

Following notification of a bomb threat, do not touch or handle any suspicious packages. Clear the area around suspicious packages and notify the police immediately. In evacuating a building, avoid windows, glass doors, and other potentially hazardous areas. Building evacuation procedures should keep sidewalks and streets to be used by emergency officials or others still exiting the building clear and unobstructed. [**730:**B.6]

N **D.6.1 Suspicious Parcels and Letters.** Be wary of suspicious packages and letters. They can contain explosives or chemical or biological agents. Be particularly cautious at high-profile facilities. [**730:**B.6.1]

Over the years, postal inspectors have identified certain characteristics that ought to trigger suspicion about a parcel, including the following:

(1) An unexpected delivery or from someone unfamiliar
(2) No return address or one that cannot be verified as legitimate
(3) Marked with restrictive endorsements, such as "Personal," "Confidential," or "Do Not X-Ray"
(4) Protruding wires or aluminum foil, strange odors, or stains
(5) City or state in the postmark that does not match the return address
(6) Unusual weight given its size, lopsidedness, or odd shape
(7) Marked with threatening language
(8) Inappropriate or unusual labeling
(9) Excessive postage or excessive packaging material such as masking tape and string
(10) Misspellings of common words
(11) Addressed to someone no longer with the organization or otherwise outdated
(12) Incorrect titles or title without a name
(13) Not addressed to a specific person
(14) Handwritten or poorly typed addresses

[**730:**B.6.1]

With suspicious envelopes and packages other than those that might contain explosives, take the following additional steps against possible biological and chemical agents:

(1) Refrain from eating or drinking in a designated mail-handling area.
(2) Place suspicious envelopes or packages in a plastic bag or some other type of container to prevent leakage of contents. Never sniff or smell suspect mail.
(3) If you do not have a container, then cover the envelope or package with anything available (e.g., clothing, paper, trash can) and do not remove the cover.
(4) Leave the room and close the door or section off the area to prevent others from entering.
(5) Wash your hands with soap and water to prevent spreading any hazardous substance to your face.
(6) If you are at work, report the incident to facility security officials, who should notify police and other authorities without delay.
(7) List all people who were in the room or area when the suspicious letter or package was recognized. Give a copy of this list to both local public health authorities and law enforcement officials for follow-up investigations and advice.
(8) If you are at home, report the incident to local police without delay.

[**730:**B.6.1]

N **D.6.2 Explosion.** In the event of an explosion, the following actions should be taken:

(1) Evacuate the building as quickly as possible.
(2) Instruct personnel to do the following:
    (a) Do not stop to retrieve personal possessions or make phone calls.
    (b) Get under a sturdy table or desk if debris and other objects are falling.
    (c) Leave quickly after debris has stopped falling; watch for weakened floors, stairs, and additional falling debris as you exit.

[**730:**B.6.2]

N **D.6.3 Fire.** In the event of a fire, the following actions should be taken:

(1) Stay low to the floor and exit the building as quickly as possible.
(2) Cover nose and mouth with a wet cloth.
(3) When approaching a closed door, use the back of the hand to feel the lower, middle, and upper parts of the door. Never use the palm or fingers to test for heat: burn-

ing those areas could impair your ability to escape a fire (i.e., using a ladder and crawling).

(4) If the door is NOT hot, open it slowly and make sure that fire or smoke is not blocking the escape route. If the escape route is blocked, shut the door immediately and use an alternative escape route, such as a window. If the escape route is clear, leave immediately through the door. Be prepared to crawl — smoke and heat rise, causing the air near the floor to be cleaner and cooler.

(5) If the door is hot, do NOT open it. Escape through a window. If you cannot escape, hang a white or light-colored sheet outside the window, alerting fire fighters to your presence.

(6) Thick smoke and poisonous gases collect first along the ceiling. Stay below the smoke at all times.

[**730:**B.6.3]

N **D.6.4 Trapped in Debris.** In the event you are trapped by debris, the following actions should be taken:

(1) Do not light a match or lighter.

(2) Do not move about or kick up dust. Cover your mouth with a handkerchief or clothing.

(3) Rhythmically tap on a pipe or wall so that rescuers can hear where you are. Use a whistle if one is available. Shout only as a last resort when you hear sounds and think someone will hear you — shouting can cause inhalation of dangerous amounts of dust.

[**730:**B.6.4]

N **D.7 Chemical and Biological Weapons.** In the event of a chemical or biological weapon attack, authorities will provide instructions on the best course of action. This can be to evacuate the area immediately, to seek shelter at a designated location, or to take immediate shelter where you are and seal the premises. The best way to protect yourself is to take emergency preparedness measures ahead of time and to get medical attention, if needed, as soon as possible. [**730:**B.7]

N **D.7.1 Chemical Weapons.** Chemical warfare agents are poisonous vapors, aerosols, liquids, or solids that have toxic effects on people, animals, or plants. They can be released by bombs; sprayed from aircraft, boats, or vehicles; or used as a liquid to create a hazard to people and the environment. Some chemical agents are odorless and tasteless. They can have an immediate effect (a few seconds to a few minutes) or a delayed effect (several hours to several days). While potentially lethal, chemical agents are difficult to deliver in lethal concentrations. Outdoors, the agents often dissipate rapidly. Chemical agents are also difficult to produce. [**730:**B.7.1]

The six types of agents are as follows:

(1) Lung-damaging (pulmonary) agents such as phosgene

(2) Cyanide

(3) Vesicants or blister agents such as mustard

(4) Nerve agents such as GA (tabun), GB (sarin), GD (soman), GF (cyclosarin), and VX

(5) Incapacitating agents such as BZ

(6) Riot-control agents (similar to Mace)

[**730:**B.7.1]

N **D.7.2 Biological Weapons.** Biological agents are organisms or toxins that can kill or incapacitate people, livestock, and crops. The three basic groups of biological agents that would be likely to be used as weapons are bacteria, viruses, and toxins. [**730:**B.7.2]

Bacteria are small free-living organisms that reproduce by simple division and are easy to grow. The diseases they produce often respond to treatment with antibiotics. [**730:**B.7.2]

Viruses are organisms requiring living cells in which to reproduce and are intimately dependent on the body they infect. Viruses produce diseases that generally do not respond to antibiotics. However, antiviral drugs are sometimes effective. [**730:**B.7.2]

Toxins are poisonous substances typically found in, and extracted from, living plants, animals, or microorganisms; some toxins, however, can be produced or altered by chemical means. Select toxins can be treated with specific antitoxins and selected drugs. [**730:**B.7.2]

Most biological agents are difficult to grow and maintain. Many break down quickly when exposed to sunlight and other environmental factors, while others, such as anthrax spores, are very long-lived. They can be dispersed by spraying them in the air, by infecting animals that carry the disease to humans, or through food and water contamination, as follows:

(1) Aerosols — Biological agents are dispersed into the air, forming a fine mist that can drift for miles. Inhaling the agent can cause disease in people or animals.

(2) Animals — Some diseases are spread by insects and animals such as fleas, mice, flies, and mosquitoes. Deliberately spreading diseases through livestock is also referred to as agroterrorism.

(3) Food and water contamination — Some pathogenic organisms and toxins can persist in food and water supplies. Cooking food and boiling water will kill most microbes and deactivate most toxins.

(4) Person-to-person — Person-to-person spread of infectious agents is also possible. Humans have been the source of infection for smallpox, plague, and the Lassa viruses.

[**730:**B.7.2]

N **D.7.3 What to Do to Prepare for a Chemical or Biological Attack.** A disaster supply kit should be assembled to include the following:

(1) Battery-powered commercial radio with extra batteries.

(2) Nonperishable food and drinking water.

(3) Roll of duct tape and scissors.

(4) Plastic for doors, windows, and vents for the room in which you will take shelter — this should be an internal room where air that can contain hazardous chemical or biological agents can be blocked out. To save critical time during an emergency, sheeting should be premeasured and cut for each opening.

(5) First aid kit.

(6) Sanitation supplies, including soap, water, and bleach.

[**730:**B.7.3]

N **D.7.4 What to Do During a Chemical or Biological Attack.** The following safeguards should be observed:

(1) Listen to the radio for instructions from authorities, such as whether to remain inside or to evacuate.

(2) If you are instructed to remain in your home, the building where you are, or other shelter during a chemical or biological attack, do the following:

(a) Turn off all ventilation, including furnaces, air conditioners, vents, and fans.

(b) Seek shelter in an internal room, preferably one without windows.

(c) Seal the room with duct tape and plastic sheeting. Ten square feet of floor space per person will provide sufficient air to prevent carbon dioxide buildup for up to 5 hours.

(3) Remain in protected areas where toxic vapors are reduced or eliminated; be sure to have a battery-operated radio at hand.

(4) If you are caught in an unprotected area, do the following:

(a) Attempt to get upwind of the contaminated area.
(b) Attempt to find shelter as quickly as possible.
(c) Listen to your radio for official instructions.

[**730:**B.7.4]

N **D.7.5 What to Do After a Chemical Attack.** Immediate symptoms of exposure to chemical agents can include blurred vision, eye irritation, difficulty breathing, and nausea. A person affected by a chemical or biological agent requires immediate attention by professional medical personnel. If medical help is not immediately available, decontaminate yourself and assist in decontaminating others. Decontamination is needed within minutes of exposure to minimize health consequences. (However, you should not leave the safety of a shelter to go outdoors to help others until authorities announce it is safe to do so.) The following steps should be taken:

(1) Use extreme caution when helping others who have been exposed to chemical agents.
(2) Remove all clothing and other items in contact with the body. Contaminated clothing normally removed over the head should be cut off to avoid contact with the eyes, nose, and mouth. Put the clothing into a plastic bag if possible. Decontaminate hands using soap and water. Remove eyeglasses or contact lenses. Put glasses in a pan of household bleach to decontaminate.
(3) Remove all items in contact with the body.
(4) Flush eyes with lots of water.
(5) Gently wash face and hair with soap and water; then thoroughly rinse with water.
(6) Decontaminate other body areas likely to have been contaminated. Blot (do not swab or scrape) with a cloth soaked in soapy water and rinse with clear water.
(7) Change into uncontaminated clothes. Clothing stored in drawers or closets is likely to be uncontaminated.
(8) If possible, proceed to a medical facility for screening.

[**730:**B.7.5]

N **D.7.6 What to Do After a Biological Attack.** In many biological attacks, people will not know they have been exposed to an agent. In such situations, the first evidence of an attack can be when you notice symptoms of the disease caused by exposure to an agent — seek immediate medical attention for treatment. [**730:**B.7.6]

In some situations, like the anthrax letters sent in 2001, people can be alerted to a potential exposure. Pay close attention to all official warnings and instructions on how to proceed. The delivery of medical services for a biological event might be handled differently to respond to increased demand. Again, it will be important to pay attention to official instructions via radio, television, and emergency alert systems. [**730:**B.7.6]

If your skin or clothing comes in contact with a visible, potentially infectious substance, remove and bag the clothes and personal items and wash yourself with warm soapy water immediately. Put on clean clothes and seek medical assistance. [**730:**B.7.6]

For more information, visit the web site for the Centers for Disease Control and Prevention, www.cdc.gov. [**730:**B.7.6]

N **D.8 Nuclear and Radiological Attack.** Nuclear explosions can cause deadly effects — blinding light, intense heat (thermal radiation), initial nuclear radiation, blast, fires started by the heat pulse, and secondary fires caused by the destruction. They also produce radioactive particles, called fallout that can be carried by wind for hundreds of miles. [**730:**B.8]

Terrorist use of a radiological dispersion device (RDD) — often called a "dirty nuke" or "dirty bomb" — is considered far more likely than use of a nuclear device. These radiological weapons are a combination of conventional explosives and radioactive material designed to scatter dangerous and sub-lethal amounts of radioactive material over a general area. Such radiological weapons appeal to terrorists because they require very little technical knowledge to build and deploy compared to that for a nuclear device. Also, these radioactive materials are used widely in medicine, agriculture, industry, and research and thus are much more readily available and easier to obtain than weapons-grade uranium or plutonium. [**730:**B.8]

Terrorist use of a nuclear device would probably be limited to a single smaller "suitcase" weapon. The strength of such a weapon would be in the range of the bombs used during World War II. The nature of the effects would be the same as a weapon delivered by an intercontinental missile, but the area and severity of the effects would be significantly more limited. [**730:**B.8]

There is no way of knowing how much warning time there would be before an attack by a terrorist using a nuclear or radiological weapon. A surprise attack remains a possibility. [**730:**B.8]

The danger of a massive strategic nuclear attack on the United States involving many weapons receded with the end of the Cold War. However, some terrorists have been supported by nations that have nuclear weapons programs. [**730:**B.8]

If there were threat of an attack from a hostile nation, people living near potential targets could be advised to evacuate, or they could decide on their own to evacuate to an area not considered a likely target. Protection from radioactive fallout would require taking shelter in an underground area or in the middle of a large building. [**730:**B.8]

In general, potential targets include the following:

(1) Strategic missile sites and military bases
(2) Centers of government, such as Washington, DC, and state capitals
(3) Important transportation and communication centers
(4) Manufacturing, industrial, technology, and financial centers
(5) Petroleum refineries, electrical power plants, and chemical plants
(6) Major ports and airfields

[**730:**B.8]

Taking shelter during a nuclear attack is absolutely necessary. There are two kinds of shelters — blast and fallout. Blast shelters offer some protection against blast pressure, initial radiation, heat, and fire, but even a blast shelter could not with-