



American Planning Association

Making Great Communities Happen

Policy Guide on Security

Adopted by the Legislative and Policy Committee, January 13, 2005

Adopted by the Chapter Delegate Assembly March 19, 2005

Ratified by the Board of Directors March 20, 2005

I. Introduction

The American Planning Association (APA) and its chapters affirm that it is imperative for planners, working in concert with first responders and other allied professionals, to:

1. actively address the causes and reduce the threats and the risks to our security;
2. support and facilitate our communities' responses to such security challenges when they do materialize;
3. facilitate the participation of all stakeholders and agencies to minimize security-related risks while not sacrificing the special physical, design, and historical character of American cities and communities;
4. maintain a balance between security and personal freedom that enhances the quality of life.

At all levels of government, planners have long been involved in decisions that affect land use relationships along with decisions that affect the design and operation of civic space, utility networks, transportation systems, and other public facilities. Planners have also been active in planning to mitigate natural hazards, disaster events, and recovery and reconstruction following catastrophes. Past planning efforts have led to the development of such concepts as defensible spaces, eyes on the street, Crime Prevention Through Environmental Design (CPTED) and the book *SafeScape: Creating Safer, More Livable Communities Through Planning and Design*. This experience and these skills can also be used to ensure best practices in security planning.

New security concerns have become a pervasive part of American life in the aftermath of the Oklahoma City bombing and the terrorist attacks that occurred in New York City, Washington, D.C., and Pennsylvania on September 11, 2001. Security measures have become a part of the landscape in nearly all American cities and communities. Public buildings and public spaces, transit and circulation points, streetscape and urban design, communications networks, and environmental and energy infrastructure systems have all been affected by security concerns.

Since 9/11, many security measures have been applied on an ad hoc basis, without regard for their impacts on development patterns and community character. Security and anti-terrorism concerns have encouraged property owners, government entities, and others to install security barriers, to limit street access, and to install a wide variety of security devices on sidewalks, buildings and transportation facilities. The short-term impacts of these measures were easily justifiable in the immediate aftermath of 9/11. Those who developed and implemented these measures should be commended for their efforts. But over time, these same installations have come to have an adverse impact upon the physical, social, economic and civic life of our communities. These long-term impacts are the issues that planners are now confronting.

As stated in *Designing for Security in the Nation's Capital*, a report prepared by the Interagency Task Force of the National Capital Planning Commission, "These installations communicate fear and retrenchment and undermine the basic premise that underlies a democratic society." As planners,

we believe that security can be combined with good practical design, and that many of these piecemeal solutions can be modified to be more comprehensive and context sensitive.

The challenge to APA and its chapters is to address security concerns while maintaining the elements that preserve and enhance great communities. At a 2004 conference titled *Safe Spaces: Designing for Security and Civic Values*, which was co-sponsored by APA, Nancy Somerville, Executive Vice President of the American Society of Landscape Architects, stated that "Security design can and should protect the public in a manner that preserves the integrity of our buildings, public spaces, and communities, while demonstrating the values of an open and accessible society."

Whether the threat to security comes from crime, from natural disasters such as floods or wildfires, or from man made disasters such as terrorism, blackouts, toxic gas emissions, or chemical spills, the planning profession should focus on the development and maintenance of safe and secure communities.

Planning for security, like planning in general, should be comprehensive. The optimal approach would cover the spectrum of potential events from natural disasters, to catastrophic events like 9/11, to events like the 1999 incident at Columbine, and to recurring events such as serious crime. The planning movement, advocating the creation of safe, defensible spaces, is a natural link to planning for the mitigation of terrorist threats.

While terrorism in the United States has led to heightened concerns over security, the security threats posed by crimes and natural disasters are much more frequent and widespread. Too much emphasis on any one of these hazards can lead to a misallocation of resources and the degradation of both the built and natural environments. In addressing most security threats, communities can often follow established planning policies and standards, such as visual openness, eyes on the street, defensible spaces, Crime Prevention through Environmental Design (CPTED), and *SafeScape*. In order to minimize the often negative community impacts of physical counterterrorism strategies, additional measures may be needed that may involve information gathering, conventional or electronic surveillance, checkpoints, and transportation or land use management measures.

At the same time, security needs should not unduly take away resources that are essential for other crucial social, economic, and physical programs. At all levels of government, the distribution of security funding should be based upon an appropriate risk assessment methodology.

Effective security planning requires collaboration among planners, architects, and other design professionals working closely with emergency managers and first responders. The experience and expertise of emergency managers and first responders, which often includes sophisticated planning and public involvement capabilities, should be made part of an interdisciplinary approach in which security needs and concerns are integrated into the overall planning process. It is equally important that basic planning concepts (e.g. eyes on the street, defensible spaces and meaningful public participation) be addressed early in the process, whenever security decisions are made.

As Americans and as members of the planning profession we assert the principle that efforts to ensure a community's safety and security should not undermine civil liberties.

As professional planners, our plans for safer communities should reflect the values of our society. In the development of plans for buildings, environments, transportation and other public facilities, the challenge for APA and its chapters is to address security concerns while maintaining the elements that preserve and enhance great communities.

From time to time, planners will have to deal with confidentiality issues and the documentation of requests for critical infrastructure information. But if a building, place, or system is unsafe, it makes more sense to fix the problem than to attempt to restrict access to information about the problem. Efforts to ensure a community's safety and security should not undermine basic civil liberties, including public disclosure and constitutional due process requirements.

APA encourages planning that will contribute to the public welfare by developing communities and environments that more effectively meet the present and future needs of people and society.

Security is more likely to be threatened in communities, and among persons, where these fundamental needs are not being met.

A policy guide on security is needed now, to help define the role of planners in security matters, and to ensure that planners are able to influence and participate in government policies and legislative decisions that involve security. It also provides a means to reassert basic planning principles and techniques that can contribute to effective prevention and mitigation of security threats.

Great communities must be safe and secure, with social equity, viable economies, cultural vitality and social diversity.

II. Definitions

In this policy guide, **Security** refers to actions taken to reduce or eliminate threats to homeland security as defined below, or to the reduction or elimination of threats posed by natural disasters or civil disorder. Other authorities restrict the use of the term "security" to refer only to hazards associated with terrorism and common crime. These authorities would use the term "safety and security" to refer more broadly to the full spectrum of risks associated with natural and manmade hazards of all types.

Homeland Security is defined as "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur." (Source: *National Strategy for Homeland Security*, White House Office of Homeland Security, July 2002.) Additionally, Executive Order 13228, *Establishing the Office of Homeland Security and the Homeland Security Council* (October 8, 2001), describes the associated functions as "detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States."

Terrorism is defined in the Code of Federal Regulations as "the unlawful use of force and/or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." (Source: 28 CFR 0.85).

As used in this policy guide, a **Threat Assessment** or a **Vulnerability Assessment** is loosely defined as "a document prepared for adoption by a public agency that assesses its vulnerability to terrorist attack or to other criminal acts intended to disrupt the public agency's operations, and that is intended for confidential distribution or for consideration in closed session." (adapted from California Government Code Section 6254 (aa)). More specifically:

A **Risk** is defined as "the potential for a loss or damage to an asset ... It takes into account the value of an asset, the threats or hazards that potentially impact the asset, and the vulnerability of the asset to the threat or hazard."

Assets are tangible and intangible resources, and **Asset Value** can be described as "the degree of debilitating impact that would be caused by the incapacity or destruction of an asset."

A **Hazard** is "a source of potential danger or adverse condition" that may be natural or manmade (either accidental or intentional) in origin, and **Threats** are a subset of hazards that generally refer to intentional actions by an adversary.

Threat/Hazard Assessment is the evaluation of threats and hazards based upon numerous characteristics such as existence, history, magnitude, and capability.

Vulnerability refers to the susceptibility of an asset to hazard damage, or, in the security context, any weakness that can be exploited by an aggressor, and **Vulnerability Assessment** is the evaluation of characteristics that contribute to and mitigate this susceptibility.

A **Risk Assessment**, therefore, is an analysis that evaluates the interrelationship between the value of an asset, the threats against it, and its vulnerability to each applicable hazard and threat. (Source: adapted from *Building Design for Homeland Security*, Federal Emergency Management Agency, 2004.)

First Responders are defined as "those individuals (including uniformed police, sheriff and fire department personnel), who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment . . . as well as emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) that provide immediate support services during prevention, response, and recovery operations." (Source: Homeland Security Presidential Directive 8, *National Preparedness*, 2003.)

Mitigation is used in this policy guide to refer to measures intended to prevent threats to security, or to minimize the potential or actual impacts of a natural or man made disaster.

Standoff distance is the distance between an asset and a threat, as defined above. The standoff distance is determined by a number of variables, including the type of threat, its assets, the desired level of protection, the type of construction, the surrounding site conditions, the site layout, the communities' intelligence gathering and communication abilities, and other community development objectives. (Source: FEMA #426 and FEMA #430).

Layers of Defense is a concept, outlined in FEMA #430, for the mitigation of potential terrorist attacks against buildings. It is also the foundation of many, if not most, strategies for the mitigation of attacks against infrastructure systems. Each layer is the demarcation point for a different set of potential security strategies. Applied to buildings:

The first layer of defense is defined as the surrounding area, including installations, infrastructure, and other buildings outside the perimeter of the site. The first layer can also include any risk management strategies such as intelligence gathering, policing, off-site operations, or management tools.

The second layer of defense includes the space and natural and physical barriers that can be introduced in the building yard to protect a particular building, typically the area between the building and the sidewalk. It includes the design and location of access points, parking, roadways, sidewalks, footpaths, water features, natural barriers, lighting, signage, and other features.

The third layer of defense refers to the building envelope itself.

In city centers or other urbanized areas, there may not be a building yard and the second and third layers of defense are one and the same.

While the concept of layers of defense, as used in FEMA #430, does not extend into the interior of a building, there are nevertheless very effective risk management strategies that can and should be employed within the interior of a building. These strategies include building programming for the secure location of valuable assets or vulnerable uses, and effective building evacuation procedures.

Crime Prevention Through Environmental Design (CPTED) is defined as "a theory of crime prevention that places a major emphasis on the design of the physical environment as the primary focus for addressing issues of public safety. CPTED relies on three primary principles: 1) natural access control, 2) natural surveillance, and 3) territoriality. Through the use of these principles, the physical environment can be modified or designed to eliminate the opportunities for a crime to be committed." (Source: *SafeScape: Creating Safer, More Livable Communities Through Planning and Design*, by Al Zelinka and Dean Brennan, published in 2001 by APA Planners Press).

SafeScape is described as an approach to designing communities that has the primary focus on creating a sense of community. In addition to changing the physical environment, the approach also involves changing how people think of and interact with the physical environment, thereby enabling

a sense of community through the design process as well as maintaining and sustaining livability (Source: *SafeScape: op. cit.* above).

Both **CPTED** and **SafeScape** are within the framework of New Urbanism design principles that are intended to facilitate integrated and fully functioning communities.

Geographic Information Systems (GIS) are defined as systems that are developed for the compilation, storage, and depiction of data through the medium of digital maps.

Global Positioning Systems (GPS) refers to sets of devices that utilize information from satellites in order to precisely define the locations of places, persons, buildings, vehicles, or other objects.

III. Security in Relation to Comprehensive Plans and Risk Management

A. Security and Comprehensive Plans

Comprehensive plans should address security once there is a thorough understanding of a community's greatest vulnerability, the acceptance of certain levels of risk and the purpose of securing a particular space, building, or precinct. Rather than be a stand-alone element, objectives and policies should be integrated into the various elements addressing land use, transportation, infrastructure or others, as appropriate. Otherwise, focusing only on security will likely cause security to trump other worthy community development objectives, and may be in conflict with APA's policy to support smart growth. Due to the changing nature and unpredictability associated with terrorism, most security measures should not be standardized or adopted into codes, at least until there is a wider body of knowledge and a normalization of the issues associated with risk assessment decision making and risk management solutions. Comprehensive plans should provide a framework on how to approach risk assessments and risk management decisions in the context of smart growth, rather than promoting incorporation, and ultimately codification, of federal risk assessment and design standards that may be narrowly focused or promote over-design.

B. The Planner's Role

There is an enormous opportunity for the planning profession to forge new ground in addressing our security needs through larger planning principles. Security policy can help to define the planner's role and help planners influence and participate in government policies and legislative decisions that involve security. It also provides a means to reassert basic planning principles and techniques that can contribute to effective prevention and mitigation of security threats.

Planners — and our fellow professional organizations that care about physical design and community building — need to articulate the difficult choices between perimeter security, mobility, accessibility, good design, and quality of life in our communities. If we truly believe that our communities and our regions should be developing according to smart growth principles, we must be willing to successfully raise these issues in the face of the short- and long-term challenges that security issues often present.

While architects and engineers have been participating in the risk management discussion in conjunction with their consulting roles, planners have been less likely to become engaged early enough in the risk assessment and risk management decision-making process. Typically, planners are presented with a set of criteria and are then asked to meet those criteria in the context of the area in which a building or facility is to be located. If planners had been involved earlier in decision-making processes, there would likely have been more opportunities to employ proven planning strategies as effective security measures.

An important role for planners is to look at security solutions comprehensively. This includes short-term and long-term solutions, cumulative impacts, and multi-faceted approaches. Planners need to seriously engage in the security dialogue to ensure that good planning and design principles be given the appropriate weight in the decision-making process and help all pertinent parties

understand the consequences of their decisions. As planners, we are obligated to inform the security community and decision makers of the full array of community objectives that should be considered when making security-related decisions.

To be effective, planners must first examine and understand underlying security needs and the array of solutions that may address these needs to facilitate the discussion about acceptable levels of risk. With this foundation, planners are in a unique position to facilitate discussion in keeping with the goal of balancing security-related objectives with community-building and development objectives.

As part of this challenge, planners can also play an active role in planning for and implementing measures that address the needs of first responders. Planners can help facilitate responses that reach across jurisdictional and organizational boundaries. Planners can push for advance planning to think about principles for first response that influence physical and operational solutions. Planners can also think about how long-term planning concepts can make first responses more effective. For example, by identifying evacuation routes in advance, our transportation planning can, over time, be more effective.

C. Risk Assessments and Risk Management

Assessing risk and determining the best risk management practices are complicated processes. Risk is often a subjective determination based on a complex interrelationship between the value of an asset, the potential threats against it, and its vulnerability to those threats, which may change over time. Consequently, risk assessments frequently address the worst-case scenarios and risk management decisions are typically narrowly focused. In a world where the tradeoffs between risk and resources have been accepted on issues ranging from highway design to air safety to vaccinations, the general public must engage in dialogue to determine the accepted level of risk posed by various terrorist threats.

Risk management or security solutions range from intelligence gathering, policing, operational procedures and site selection and design (building to landscape or streetscape design) to larger planning-based solutions such as transportation and land-use management. Physical security solutions typically rely on large standoff distances (building setbacks) or promotion of secure campus-style development in less developed locations, along with limits on vehicular access and, in some cases, pedestrian access. Physical security solutions also involve prohibiting or discouraging activated ground-floor uses and placement of closely spaced barriers around the perimeters of buildings, typically within and adjacent to public space.

While most of these solutions may help to prevent progressive collapse and avoid mass casualties in the facilities — often the primary goals in counterterrorism design — none of these solutions will prevent terrorism nor prevent collateral damage caused by a massive explosion. Even if security barriers are placed around a building, and even if the building is structurally sound, death and injury can occur blocks away from the source of the blast due to flying debris and broken glass.

At present, larger planning strategies are not typically considered in the decision-making process, but are a reaction to, or consequence of, physical or design-based solutions. Accordingly, physical counterterrorism security is being addressed building by building, and at the very best at the scale of a block, not at the scale of a precinct or city, which may be more appropriate in some situations. For example, large standoff distances are typically impossible to meet in city centers; therefore, an entity can either accept additional risk or relocate to an outlying area. However, there may be other viable solutions, such as operational procedures or transportation management. Risk can be reduced by restricting the location of certain types of vehicles in high-risk areas at certain times. Delivery trucks could be screened off site and accompanied to their destination, or vehicle type and size could be restricted in high-risk areas during certain times of the day.

Terrorism can take many forms, including hijackings, biological attacks, and hostage executions; however, bombing (pipe bombs to large container explosives) are the most prevalent form of terrorism because delivery of the threat is relatively easy to execute. With the exception of the horrific events of the Oklahoma City bombing and the World Trade Center, terrorism aimed at Americans has been primarily directed at military or diplomatic mission facilities overseas. But in

countries where terrorism is more prevalent, the targets are often places that are not owned or used by a government, such as restaurants, clubs, and other types of entertainment facilities.

D. Careful Use of Guidelines and Standards

In response to terrorist attacks on our citizens and military in the past 15 years, counterterrorism security has become a predominant part of our everyday lives, especially in the nation's capital and in large cities such as New York. Understandably, the standards and operational procedures that have been developed to date are in response to the most significant terrorist events. The primary physical-based standards were developed by the Department of State (DoS), the Interagency Security Committee (ISC), and the Department of Defense (DoD). The standards were intended to protect diplomatic foreign missions in areas where terrorism has been prevalent, large federal office buildings located throughout the country, and military installations and ancillary uses.

Application of the security measures developed by and for the federal government is profoundly changing the character and form of our communities and metropolitan regions. The ISC's level of protection standards for most federal office buildings requires large setbacks, a minimal mix of uses (if any at all), and restricted parking. These limitations will result in disconnected, isolated development patterns, leading to the relocation of office space from city centers or urbanized areas to secure campuses in outlying locations. The nature of physically based counterterrorism risk management solutions is, for the most part, the antithesis of smart growth. The negative impacts of these solutions on smart growth objectives are apparent; these measures act as disincentives to compact urban development forms, accessibility, lively public spaces, and mixed-use communities.

Overall, risk assessment and risk management standards (physical design tools, operational strategies, and other guidelines) are still in the early stages of development and implementation. It is important to recognize and identify both the value and the limitations of different documents that are being used to develop de-facto standards in both the public and private sectors.

There is not a one-size-fits-all solution for security. New threats and their methods of delivery continue to emerge; new technologies to reduce vulnerability continue to be developed; and the understanding of the threats, solutions and the associated trade-offs that are inherently part of the risk assessment and risk management decision-making process are improving.

While the documents referenced in this policy guide contain very useful information, are a valuable resource, and should be used when planning and designing for security, even the best of these resources are being continuously evaluated and best practices refined based on lessons learned in this emerging field. New strategies continue to be identified, studied, developed and tested for potential effectiveness.

IV. Overview of Legislation, Regulations And Standards

A summary of legislation, regulations, and standards affecting homeland security is attached to this policy guide as an appendix. With respect to the policies that are included in this guide, the essential pieces of federal security legislation include:

- The *Robert T. Stafford Disaster Relief and Emergency Assistance Act* ("Stafford Act," Pub. L. 93-288, as amended) "was enacted to support state and local governments and their citizens when disasters overwhelm them. This law establishes a process for requesting and obtaining a Presidential disaster declaration, defines the type and scope of assistance available under the Stafford Act, and sets the conditions for obtaining that assistance." (Source: DHS)
- The *Disaster Mitigation Act of 2000* ("DMA 2000," Pub. L. 106-390) amended the *Stafford Act* by repealing the previous mitigation planning provisions (§409) and replacing them with a new set of requirements (§322) that emphasizes the need for state, tribal, and local entities to closely coordinate mitigation planning and implementation efforts and links the planning requirements to eligibility for several categories of disaster recovery funding.

- The *Homeland Security Act of 2002* (Pub. L. 107-296) established the United States Department of Homeland Security.
- The *Critical Infrastructure Information Act* (the "CII Act," Title II, Subtitle B of the *Homeland Security Act of 2002*) "regulates the use and disclosure of information submitted to ... DHS about vulnerabilities and threats to critical infrastructure." (Source: Congressional Research Service)

The *Disaster Mitigation Act of 2000* (Pub. L. 106-390), or DMA 2000, represents a shift in public policy from disaster response to mitigation, including mitigation planning to prepare for and avoid disasters. Included among the federal requirements for DMA 2000-compliant local, state and tribal multi-hazard mitigation plans is the development of a risk assessment that provides the factual basis for developing a mitigation strategy. The risk assessment requirements are promulgated in 44CFR201.4(c)(2) for state plans and 44CFR201.6(c)(2) for local plans. (Tribal plans can be developed to meet either state or local requirements.) DMA 2000 deals primarily with natural disasters, but its principles can easily be extended to include manmade hazards involving system failures and homeland security.

In connection with the establishment of the Department of Homeland Security (DHS), Executive Order EO-13284 amends a number of earlier Executive Orders and establishes the functions of certain officials in the DHS.

In matters related to planning for security, Executive Order EO-12372, entitled "Intergovernmental Review of Federal Programs," requires that "... federal agencies shall provide opportunities for consultation by elected officials of ... state and local governments." EO-12372 further requires that federal agencies shall "communicate with state and local elected officials as early in the program planning cycle as is reasonably feasible to explain specific plans and actions."

A number of Executive Orders, from the Kennedy Administration through to the Clinton Administration, have established and maintained the federal policy of locating federal facilities in center cities and urban districts. Executive Order No. 12072 was issued during the Carter Administration on August 16, 1978.

The Department of Defense (DoD) has published Unified Facilities Criteria (UFC) 4-010-01 (version 8 October 2003), entitled "Minimum Antiterrorism (AT) Standards for Buildings." UFC 4-010-01 includes 23 standards in four major categories: site planning, architectural, structural, and electrical/mechanical. These DoD standards establish a regime that includes minimum standoff distances (i.e. building setbacks and clear areas) as the "primary strategy" for the protection of buildings and facilities used by the military (Source: *The Military Engineer No. 622* March-April 2003, p. 36).

In 1995, the Department of Justice issued a report entitled *Vulnerability Assessment of Federal Facilities*. This report addressed security levels and minimum-security standards for federal office buildings. It also included a recommendation to create the Interagency Security Committee (ISC) as a permanent body to develop long-term construction standards for locations requiring blast resistance or other specialized security measures, as well as to address continuing government-wide security issues.

The ISC has prepared three guiding documents that contain physical security, design, and construction criteria for new, renovated, or leased federal buildings: 1) *New Federal Office Buildings and Major Modernization Project*, 2) *Minimum Standards for Federal Building Access Procedures*, and 3) *Security Standards for Leased Spaces*. These documents are performance-based and should be applied as such.

According to the GSA Office of the Chief Architect (OCA), "the ISC (has) revised and updated GSA's 1997 Draft Security Criteria, taking into consideration technology developments, new cost considerations, the experience of practitioners applying the criteria, and the need to balance security requirements with public building environments that remain lively, open, and accessible ..." Further, the ISC "developed the ISC Security Design Criteria to ensure that security becomes an

integral part of the planning, design, and construction of new federal office buildings and major modernization projects."

In response to the proliferation of unsightly barriers throughout the nation's capital, the National Capital Planning Commission, the planning and review agency for the federal government in the National Capital Region, prepared the *National Capital Urban Design and Security Plan*. The plan establishes a framework and provides guidance on how to plan and design building perimeter security to integrate it into urban landscapes and minimize the impact to the public realm. While the plan was developed to address the concentration of federal facilities in Washington's urban core, it has also served as a model for other communities that face similar challenges.

Additionally, the GSA-OCA has developed a technical pilot report for Perimeter Security for Historic Buildings. Also, GSA is currently working on a perimeter security handbook that will be completed in the coming year.

In addition to guidance on the implementation of DMA 2000, FEMA has also issued a series of publications in its Risk Management Series (RMS). While not part of an official federal policy, FEMA's RMS publication #426 embodies an approach to mitigating manmade disasters that is intended to be more context-sensitive than the more prescriptive DoD approach, as exemplified in DOD UFC 4-010-01, for reasons which are explained below.

Additional RMS publications are forthcoming from FEMA, including a primer (FEMA #430), being prepared with the collaboration of the National Capital Planning Commission (NCPD), which will address building, site, and design guidance to mitigate potential terrorist attacks. Other forthcoming design guides will address the protection of public buildings from natural disasters such as earthquakes, floods, and high winds.

The dissemination of public infrastructure information has been restricted pursuant to several federal laws and regulations, including Presidential Decision Directives (PDD-) 62 and 63, both of which were issued in 1998. PDD-63 established the National Infrastructure Protection Center (NIPC) at the FBI, to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against critical infrastructures (source: National Academies Press).

6 CFR Part 29 designates "Protected Critical Infrastructure Information (PCII)," and protects it from disclosure under a specified exemption to the Freedom of Information Act. 18 CFR Part 388 applies to the restriction of access to Critical Energy Infrastructure Information (CEII), and 49 CFR Part 15 defines the category of "Sensitive Security Information (SSI)" in relation to transportation infrastructure.

The Federal Geographic Data Consortium has issued *Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns*. Also, the Rand Corporation has published *Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information*.

At the state and local levels, public records laws are being changed to protect critical infrastructure information. For example, the North Carolina Public Records Law was amended in January 2002. Under the amended state law, information "containing specific details of public security plans and ... the detailed plans and drawings of public building and infrastructure" is no longer considered public information and can be restricted. Pursuant to the amended state law, the City of Greensboro enacted its own Infrastructure Information Security Policy, with an effective date of July 1, 2004. Alaska and Utah have enacted similar legislation.

V. Policies

1. The General Need for a Planned Approach

APA and its chapters support security and emergency management planning that is integrated with overall community development objectives, in order to achieve a balanced approach. Security and emergency management planning should be comprehensive and should not rely solely on physical security measures building by building. Planning for security should include intelligence and information gathering along with assessments of state and local government administration, operations, infrastructure, transportation, and land use management. Security solutions should be applied at an appropriate scale, *e.g.* a building site, a block, a street, or a precinct.

Reasons to Support

Planning is a broad-based profession that looks at linkages, synergies and social, political, and economic ecologies. We tend to favor the wide perspective and the long view of time. A hodge-podge of hasty solutions (*e.g.* jersey barriers, expanded perimeters, street closings, etc.) can mar the historic fabric and good design of many of our American cities and towns. Uninformed security policies could have harmful effects such as exacerbating sprawl and unforeseen locational impacts. It is important to view security in a broader context, and the implications of its application unilaterally within society. Security policy and planning should be linked to the larger concept of great communities. Security should complement, not pre-empt community life. Life is a continuum and security is part of that continuum.

2. Crime Prevention Through Environmental Design (CPTED) and SafeScape

As the primary means for advancing security objectives, APA and its chapters affirm their support for approaches to planning that promote a sense of community, encompassing public involvement activities, defensible spaces, and "eyes on the street." Two of the more comprehensive approaches in this category are Crime Prevention Through Environmental Design (CPTED) and *SafeScape*, both of which are defined in Section II, above. There are many individual planning measures that have been shown to enhance security, including design controls, natural surveillance, natural access control, territoriality, good lighting design, and others. These planning measures can address vulnerability and risk in a more effective manner than have many of the post 9/11 ad hoc measures, which heighten fear and unduly compromise the unique character of a place and of a community.

Reasons to Support

This policy is needed in order to ensure that there is a reasonable balance between planning for crime prevention and planning to mitigate acts of terrorism. Acts of terrorism are infrequent events, and everyday crime levels may increase further if security measures are enacted that undermine the integrity of a community. Measures that may undermine a community would include street closures, rigid adherence to arbitrary standoff distance standards, etc. More flexible standards would allow response to increased or reduced threats on an "as-needed" basis.

3. State and Local Policies Affecting Building Locations and Orientation, Street Closures, and the Public Realm

At the local level, APA and its chapters shall promote the adoption and implementation of security planning policies that enable communities to implement strategies fostering smart growth.

In the development of security plans and plans for safe growth and safe communities, APA and its chapters advocate security policies and guidance that focus on: (1) performance rather than prescriptive standards that address physical, operational, and other approaches, and that are context-appropriate; (2) balancing security and overall community development objectives; (3) responses that reflect different scales: site, neighborhood, community, and region; (4) strategies that develop and incorporate community-based risk assessments in addition to specific assessments; and (5) incorporating new information about new security threats and new technology and security solutions.

Reasons to Support

Sound planning and mitigation is the most cost effective approach to achieve a given level of security. It is the only practical strategy for dealing with the existing built environment. The integration of risk and vulnerability assessments and mitigation techniques into the planning process also ensures the safest possible overall environment within a community.

4. Policies and Standards Affecting the Location and Design of Federally Owned or Leased Facilities.

APA and its chapters support the establishment of federal building location standards that are consistent with existing federal policies that encourage placement of federal facilities in urban locales and near transit. These standards are preferable to more prescriptive standards, which rely on minimum standoff distances as the "primary strategy" for the protection of buildings and facilities. More flexible and dynamic standards would be more consistent with smart growth planning principles and would be more effective in maintaining a sense of community within developed areas.

For civilian applications in urban areas, the building location and design standards recently enacted by the DoD do not provide sufficient flexibility with regard to standoff distances (i.e. building setbacks), barriers, and parking. Security standards issued by the ISC and the GSA are more flexible, but they are also prescriptive in nature and are based on threat levels that are not realistic for most localities.

For siting federally owned or leased facilities, APA and its chapters support the adoption of federal policies that are consistent with the preceding policy regarding state and local policies (Policy Number 3).

Specifically, federal policies for the location and design of federally owned or leased buildings should focus on (1) performance rather than prescriptive standards that address physical, operational, and other approaches, and that are context appropriate; (2) balancing security and overall community development objectives; (3) responses that reflect different scales: site, neighborhood, community, and region; (4) strategies that develop and incorporate community-based risk assessments in addition to specific assessments; and (5) incorporating new information about new security threats and new technology and security solutions.

Reasons to Support

If they are too rigidly applied, or if they are applied outside of the context of an overall facility master plan, prescriptive standards, including recently enacted DoD standards, may have the potential for forcing unintended dispersion, sprawl, or land consumption, and they may conflict with existing federal policies that encourage the location of federal facilities in center cities and urban districts (e.g. Executive Order 12072, enacted in 1978). Prescriptive standards could also lead to the prohibition of federal leasing in walkable or transit-served locations.

Standardized, prescriptive, federal security standards may conflict with local ordinances and with initiatives based on sound planning principles. For example, they could have the potential for forcing unintended dispersion or sprawl. They may also detract from existing Federal policies that do encourage the location of federal facilities in center cities and urban districts.

If federal buildings are located or designed in accordance with standards that are different from the generally prevailing standards in a district or neighborhood, then federal buildings will become more conspicuous as potential targets for terrorist attacks.

While there may be security benefits associated with the dispersal of public buildings, the same benefits can also be achieved through other measures that are less likely to require sprawl or excessive land consumption. For example, the provision of backup systems in outlying locations can ensure continuity of system operations without disrupting normal urban activities and interactions.

5. Security Planning for Transportation Facilities and Services

APA and its chapters support the planning and implementation of vehicular and pedestrian evacuation routes balanced with community objectives as an element of comprehensive security plans involving the location and orientation of buildings and public spaces.

Further, APA and its chapters advocate the development of security provisions that enable communities to implement smart growth strategies and transit oriented development without undue design constraints. To this end, APA and its chapters shall:

- Promote research on best practices for security planning for transit facilities, addressing specific physical security provisions related to stations, boarding areas, bus stops, and the surrounding public realm.
- Promote flexible development standards relative to density, minimum setbacks, shared parking, on-street parking, and ground floor retail uses, consistent with a regularly updated and site-specific risk assessment strategy.
- Promote good road design, street connectivity, and the use of streetscape elements in the public realm as part of an overall community security plan.
- Promote the adoption and implementation of "Safe Walk to School" programs in upcoming federal transportation legislation, along with similar state and local initiatives that are intended to facilitate pedestrian travel and to protect and enhance pedestrian safety.
- Promote flexibility in developing landscape design guidelines that address the need for balancing screening and providing visibility to a specific site.

Reasons to Support

The placement of physical barriers outside buildings, the closing of urban streets, and the rigid application of standoff distance standards, may all lead to situations that interfere with the safe evacuation of buildings and urban places. Evacuation routes must be planned concurrently with planning for street closures and for the location and design of physical barriers outside buildings.

Standards that require either the physical separation of buildings or the elimination of ground level storefront activities may interfere with pedestrian circulation, access to transit facilities, and the principle of "eyes on the street." Examples from New York City as it plans new transit facilities in Lower Manhattan and elsewhere should be examined for the use of new techniques and alternatives.

6. General Security Planning Policy for Public Facilities

APA and its chapters endorse the adoption of a security planning process for public facilities that provides a comprehensive focus on prevention, protection, response, and recovery/continuity beyond traditional plans. Each of these factors has a different set of planning considerations.

Prevention discourages criminal or terrorist activities through streetscape and site-specific design provisions consistent with the tenets of Crime Prevention Through Environmental Design (CPTED), *SafeScape*, and APA "Growing Smart" initiative. This is generally governed by comprehensive and neighborhood planning.

Protection measures, such as those contained in *The National Capital Urban Design and Security Plan*, ensure that the design of the public realm and individual buildings minimize the destruction of people and property in the event of an incident. This is generally governed by site plan guidelines and building codes.

Response is affected by the location and protection of critical infrastructure and appropriate plans for shelter and evacuation of staff and the public. It is also affected by training and a clear chain of command involving first responders.

Recovery and continuity plans ensure that essential public services can continue unabated in the event of a security emergency. They include not only transportation, public health and safety services, but also counseling, public information and referral, essential contractors, and vendors that provide public services.

Reasons to Support

Planning for security is still new in many areas of the United States. Until basic security planning

principles are well understood and widely applied, there is a risk that security measures will be enacted that are either counterproductive or needlessly disruptive of normal community activities. To be effective, planning for security should include some heretofore non-traditional planning considerations.

7. Building Design for Security

APA and its chapters support the development of building, zoning, and urban design guidance that promotes general security objectives while balancing community objectives, particularly as this guidance relates to:

- Parking Facilities, Including Garages
- Vehicular and Pedestrian Circulation
- Landscaping
- Lighting
- HVAC Systems
- Entry Ways and Access Points
- Lobbies
- Elevators and Stairwells, and
- Delivery Docks.

APA and its chapters also support consideration for the expansion of the scope of building codes in order to address security measures related to the location and design of features such as windows, doors, mail and utility rooms, closets, trash bins, and communications and computer systems. Such measures should also be balanced with community objectives.

The review of existing building codes should address both building access and the quick and orderly evacuation of buildings.

APA and its chapters recommend that localities undertake a comprehensive review of their development review and permitting processes in order to adopt measures, policies, and regulations that could reduce the likelihood and mitigate the effects of criminal activity. Such measures can also be helpful to reduce fear of criminal behavior as well as the actual incidence of criminal behavior, and they can be viewed as a means for fostering safe growth within communities.

Reasons to Support

Compliance with building code requirements adopted before 9/11 may no longer be a good defense to liability claims based on the building owner's failure to take steps to protect persons on the premises. Due diligence in the acquisition of existing structures also requires consideration of physical security factors. Such considerations must also be a factor in redevelopment, retrofit, and remodeling decisions.

Planners, architects, developers and building owners must work together to take security measures into consideration in the planning, design, and permitting process. Measures to promote physical security should not be left solely to the discretion of the security community. The challenge for planning and security is to develop a process and regulations that realistically integrate both processes and bodies of knowledge.

8. Incorporation of Security Issues into the Comprehensive Planning Process

In planning for the reduction of both natural and man made risks, APA and its chapters advocate the inclusion of a range of security measures into local and regional planning programs. Following the approach that is generally outlined in APA "Growing Smart" initiative, planners should work to ensure that local comprehensive plans include the planning and design of community infrastructure and land uses that reduce threats to the public health, welfare and safety of communities. Security policies should be integrated into the various elements of a comprehensive plan addressing land

use, transportation, infrastructure or other issues as appropriate. Comprehensive plans should provide a framework on how to approach risk assessments and risk management decisions in the context of smart growth, and communities should consider incorporating the results of threat, vulnerability, and risk assessments directly into comprehensive plans, administrative policies, capital budgets, and the regulatory process.

Planning for security should also involve planning for energy resources and systems.

The National Capital Urban Design and Security Plan, published by the National Capital Planning Commission for Washington DC, is recognized as a prototype for the incorporation of security principles into the comprehensive planning process.

In states that have comprehensive planning requirements, APA and its chapters support the inclusion of security as one of the required elements.

Reasons to Support

Aside from certain federal agencies including the DoD, safety and security planning have yet to be institutionalized and incorporated into the planning process through plans and regulatory documents. Processes, procedures, and model language still need to be developed.

9. Use of GIS and Related Technologies

APA and its chapters endorse additional federal support for the development of coordinated and accessible GIS and related data and applications, recognizing the federal government's current role as the most important source of geographic and remote sensing data.

APA and its chapters also support the adoption of state and local policies and procedures that will facilitate the sharing of geospatial data, along with GIS and GPS-related technological expertise, among planners and first responders for security purposes.

Reasons to Support

The field of planning relies heavily on good geospatial data. From parcel data to floodplain contours, the activity of planning uses geographically based sources of information to provide a basis for better decision making. This has led to the increased use of GIS software, such as ESRI's ArcGIS and others.

Planning as a profession is accustomed to working with large complex data sets and to using GIS and similar software to model various phenomena and to analyze scenarios. Examples of urban modeling software include Community Viz, What If? and UrbanSim.

Planners often have access to local land use, building, and development data and technical resources that can be crucial to prevention, preparedness, response, recovery, and mitigation activities. However, anecdotal evidence suggests that planners and first responders do not easily exchange data and information, whether in day-to-day transactions or in crisis situations. Policy and technical strategies to improve these connections should be developed, especially since we know that reliance on technologies such as GIS, GPS, and related planning information systems is growing rapidly in local jurisdictions across the United States and that these are vital tools in crime and crisis management.

10. Coordination with First Responders

In matters related to security policies and plans, APA and its chapters support closer coordination of local and regional planners with emergency managers and first responders including police, fire, and emergency medical staffs. APA and its chapters are committed to elevating the level and quality of discourse and communication between planners and first responders in routine, local, and regional level planning activities. The public interest would be better served by planners who are better educated in security matters, as well as by enhanced, more stable, and better informed working relationships between planners and first responders.

Reasons to Support

Recent incidents — from terrorist attacks to school violence — provide more imperatives than ever for planners, police, fire, and medical first responders to communicate effectively and work together in smarter ways. Despite this, these groups collaborate unevenly in local jurisdictions across the United States and, based on anecdotal evidence, it appears that their communication and understanding of each other's roles relative to security planning are less than optimal.

Planners, architects, developers, building owners, emergency managers, and first responders must work together to take security measures into consideration in the planning and permitting process. Measures to promote physical security should not be left solely to the discretion of first responders. The challenge for planning and security is to develop a process and regulations that realistically integrate both processes and bodies of knowledge. Planners should contact their local law enforcement agencies to see what training opportunities are already available at the local level.

11. Federal, State, and Local Consultation

In matters related to planning for security, federal and state agencies are encouraged to utilize locally adopted land use approval processes, including comprehensive plan, zoning, site design and design review. APA and its chapters support the more consistent and effective enactment of Executive Order EO-12372, entitled "Intergovernmental Review of Federal Programs." EO-12372 requires that "... federal agencies shall provide opportunities for consultation by elected officials of ... state and local governments." EO-12372 further requires that federal agencies shall "communicate with state and local elected officials as early in the program planning cycle as is reasonably feasible to explain specific plans and actions."

Reasons to Support

In response to emerging concerns regarding terrorism, federal agencies and officials have become more involved in planning decisions that have been previously left to state and local governments. Local planners should also become more involved at the federal level. In the wake of these redefined relationships, the need becomes more urgent for more effective coordination among federal, state, and local officials. The Oklahoma City survivors have spoken to these needs with uncanny applicability to WTC and natural disaster response.

12. Threat, Vulnerability and Risk Assessments

In the preparation of threat, vulnerability, and risk assessments, APA and its chapters support the development of community-based planning strategies and design guidelines that provide guidance on how the physical environment can be designed or retrofitted in response to a threat assessment or identified threat level. These standards should be based upon risk assessments that reflect the specific needs of the community.

A one-size-fits-all approach to vulnerability assessments risks the misallocation of public and community resources. With careful attention to the principles of good urban design, the concept of layers of defense can help to minimize the potentially adverse impacts of physical barriers, minimum standoff distance requirements, and other similar methods.

APA and its chapters further support the development and adoption of:

- advanced methodologies for conducting threat and vulnerability assessments at the building, site, and community levels;
- best practice standards for the mitigation of threats at the building, site, and community levels; and
- procedures for the review of subdivisions and site plans that incorporate consideration for threat and vulnerability assessments and risks, along with consideration of requirements for emergency response and for the continuity of operations.

Reasons to Support

Planners have a significant role to play in planning for crime prevention and security. Threat and

vulnerability assessments will be flawed if they do not incorporate basic planning principles. On the other hand, comprehensive plans and building codes will be deficient if they do not account for the findings derived from threat and vulnerability assessments.

13. Access to Public Meetings and Records

As current and complete information on the natural and built environment is critical to the effectiveness of planning, it is the policy of APA and its chapters that the planning community should participate in confidentiality determinations and the classification of critical infrastructure information. APA and its chapters affirm that the protection of civil liberties and personal freedoms must be upheld. APA and its chapters also recognize that security requirements may sometimes make it necessary to protect public disclosure of certain information regarding public meetings, documents, and data, including digital and printed maps, GIS databases, and other geospatial data.

A) State and Locally Imposed Public Access and Disclosure Restrictions

Effective community planning depends on the engagement of an informed public. It is the policy of APA and its chapters that all geospatial information remains in the public record, with exceptions provided for specific data attributes that are traditionally kept confidential, such as the number of employees in a building or at a site. In specific instances where a significant threat to homeland security has been clearly established, and in order to minimize threats to homeland security, APA and its chapters support the enactment of state and local legislation and regulations that may protect access to and disclosure of critical data (including geospatial data) and public documents. Whenever public access is thus restricted, the restrictions themselves shall be clearly defined and officially adopted on behalf of the relevant government bodies.

Unless there is an imminent emergency involving the potential loss of many lives, these restrictions should not be applied on an ad hoc basis. These restrictions should only apply in instances where there is a serious potential threat to security that clearly outweighs the ongoing need for public discourse or the disclosure of public information.

APA and its chapters endorse procedures that involve layers of confidentiality, with different standards and requirements imposed at different layers (e.g. low-level, mid-level, and high-level confidentiality).

Notwithstanding these restrictions, planners themselves should be encouraged to participate in closed public meetings whenever they involve subjects pertinent to the planners' professional expertise or experience.

Given that the essential purpose of a threat or vulnerability assessment may be compromised if its contents were made available to the public, APA and its chapters support the enactment of state and local legislation and regulations that are intended to restrict access to confidential infrastructure information. It is essential that planners themselves be directly involved in developing assessments pertaining to natural, manmade, or terrorist risks whenever these assessments point to the need for changes in the planning, design, or engineering of buildings or public facilities.

B) Clearances and Confidentiality Agreements

APA and its chapters encourage professional planners to seek out and obtain whatever clearances and authorizations may be needed in order to ensure that they are authorized to have access to critical documents and meetings without unduly compromising security objectives. In furtherance of these security objectives, planners shall also be encouraged to execute confidentiality agreements.

C) Documentation of Requests for Critical Infrastructure Information

Disclosure and documentation of requests for critical infrastructure information must follow procedural guidelines that have been drawn up in conformance with federal and state laws

establishing requirements for open meetings, public disclosure, freedom of information, and an individual's right to privacy.

If, and only if, relevant procedural guidelines have been officially enacted by his or her employer pursuant to established applicable due process requirements, APA and its chapters encourage public sector professional planners to systematically document requests for critical infrastructure information. Subject to individual state freedom of information and privacy laws, a typical list of information pertaining to such a request might include:

- the name of the person receiving the request,
- the name and birth date of the requestor,
- a copy of the document used for confirmation of the requestor's identity (e.g. a driver's license),
- the date of the information request,
- a description of the data requested,
- an explanation of the given need for the requested information, and
- a summary of the action(s) taken by the person who received the request.

Reasons to Support

At the local level, communities are struggling with the conflicting needs of maintaining data security while encouraging open participatory government. Planners need to be leaders in these discussions. APA and its chapters will remain vigilant in defense of the public's right to fully participate in decisions affecting the fabric of their communities.

On a daily basis, planners interact with and release to the public, information that is potentially useful to terrorists. Public bidding and open and competitive processes are the hallmark of the planning profession, yet access to bid documents, plans, or utility layouts, for example, may give terrorists just what they seek.

14. Allocation of Public Funds

APA and its chapters support the development of a national strategy that sets minimum standards for the protection of all citizens while concentrating funds and energy on areas at highest risk, for the purpose of allocating scarce resources among competing funding priorities. In partnership with federal agencies including, but not limited to, the Department of Homeland Security, state and local governments must play a direct role in the development of an appropriate risk-assessment strategy.

The distribution of scarce funding without a systematic analysis of need, population, and threat, must be addressed at all levels of government, as well as by a number of different federal departments and agencies that are involved with security. These departments include the Department of Homeland Security, the Department of Transportation, and the Department of Housing and Urban Development.

Additional public funding is required in order to achieve more effective coordination among planners, design professionals, and first responders.

Additional public funding is also needed for the further development and implementation of new technologies for security planning, including remote sensing, visioning, scenario building, and GIS technologies.

Reasons to support

Although all communities may face threats, there are critical areas of the country that are at the highest risk from terrorist attack. Attention and funds should be concentrated on those areas, cities, and important symbols that are at highest risk.

In the rush to allocate funds for homeland security subsequent to 9/11, severe imbalances have developed between the need and availability of scarce federal funding resources. Current mechanisms are inadequate for the task and are subject to political abuses. In order to achieve an optimal level of homeland security, better funding allocation methods are currently under development. In furtherance of the objectives of our profession, APA needs to line up in support of the development and application of these measures.

We are encouraged by recent commitments that have been made regarding the allocation of federal homeland security funds. These commitments were made to a House appropriations subcommittee on behalf of the Department of Homeland Security, by the incoming Homeland Security Secretary Michael Chertoff who said, "Our philosophy, our decision making, our operational activities and our spending must be grounded in risk management as we determine how to best organize to prevent, respond, and recover from attacks." Rep. Harold Rogers, the chairman of the subcommittee, responded, "Whether you are from rural or urban areas, we want the money distributed based on an objective assessment of the risk and the threat." (Source: *The New York Times*, March 3, 2005).

15. Education and Research

APA and its chapters support new initiatives in the development of a wide range of professional development resources regarding security through APA publications, sponsored research, and support for conferences and symposia focused on security.

Specifically, APA and its chapters support the initiatives being undertaken regarding security as a principal component of APA's *Safe Growth America Initiative*, including the forthcoming *Safe Growth Reader*. These initiatives will allow APA to take a leadership role in education of planners, planning commissions, zoning officials, local government officials, and the public on the elements of site and building design in relation to security issues.

Continuing education and outreach efforts should include the preparation and release of additional Planning Advisory Service Reports, and the development of new courses that train citizen and professional planners to properly formulate and integrate security programs into the planning process.

In instances where states develop continuing education requirements for citizen and professional planners, APA and its chapters support the inclusion of security and crime prevention planning as required elements.

Planners and development representatives are encouraged to seek training through their local and state crime prevention associations, in order to learn more about CPTED, *SafeScape*, and other crime prevention planning and design strategies.

APA and its chapters support specific research on interactions of local planners with police, fire, and emergency medical staff relative to security policy and plan-making processes. The research should document interactions relative to first response as well as to subsequent mitigation achieved through planning.

Reasons to Support

Research and education are two of the most important components of any coordinated management plan. Information sharing on all levels will encourage cooperation between those mitigating disasters or responding to adversity.

In planning for security, coordination of planners, first responders, federal, state, and local agencies requires first that all participants are equally aware of the factors affecting sound decisions in the face of a disaster. Research and education are two of the most important components of any coordinated management plan. Information sharing on all levels will encourage cooperation between those mitigating disaster threats or responding to adversity.

The use of available research, training resources, and continuing education will enable citizen and professional planners to play a more active role in security planning, will accelerate the

implementation of planning processes that take planning for security into account, and will foster support for security planning among public officials, developers, engineers, first responders, and other allied professionals.

VI. Next Steps

Although new attention has been focused on security planning in the aftermath of 9/11, the basic planning principles and relationships are not that new. Established approaches to planning have already been developed that are intended to reduce the likelihood and consequences of crime, catastrophic accidents, and natural disasters, including earthquakes, fires, floods, hurricanes, tornadoes, and other weather-related events. Future policy guides should be developed that will be more closely focused on planning in relation to these types of risks.

DMA 2000 (Pub. L. 106-390) focuses on mitigation planning for natural disasters. Since 9/11, FEMA has encouraged state and local jurisdictions to consider manmade threats along with planning for natural disasters. This encouragement has included the development of numerous publications in the FEMA Risk Management Series. Along with the inclusion of FEMA as a part of the Department of Homeland Security, these initiatives suggest that planning for security is essentially similar to planning for responses to natural disasters. APA and its chapters support this position.

The solutions to these issues are programmatic as well as physical. The best solutions are those that have community participation in the planning and implementation of the recommendations. Planning, land use, and design decisions can play a major integrative and facilitative role in achieving these results. Consideration of multiple objectives will create greater economic efficiencies and improve the quality of security by optimizing the participation of a community in its own security.

As noted above, as part of the policy on education and research (Policy Number 15), APA and its chapters support the preparation and release of additional Planning Advisory Service (PAS) reports pertaining to security, along with the development of new courses that train citizen and professional planners to properly formulate and integrate security programs into the planning process, as part of APA's *Safe Growth America Initiative*.

VII. Selected References

Zelinka, AI, and Dean Brennan. *SafeScape: Creating Safer, More Livable Communities Through Planning and Design*. 2001. Chicago: APA Planners Press.

National Capital Planning Commission. 2001. *Designing for Security in the Nation's Capital*.

National Capital Planning Commission. 2003. *The National Capital Urban Design and Security Plan*,

FEMA 426. 2003. *Reference Manual to Mitigate Potential Terrorist Attacks*.

FEMA 430. forthcoming 2005. *Building, Site and Layout Design Guidance to Mitigate Potential Terrorist Attacks*.

Calhoun Young, Rufus, and Dwight H. Merriam. "Homeland Security Begins at Home: Local Planning and Regulatory Review to Improve Security" in *Land Use Law & Zoning Digest*. November 2003.

National Conference of State Legislatures. 2003. *Protecting Water System Security Information*.

Appendix

Overview of Legislation, Regulations, and Standards

The legislative foundations of what is now homeland security in the United States date back to the beginning of the Cold War. Key pieces of legislation include the following:

- The *National Security Act of 1947* (Pub. L. 80-253) reorganized foreign, military, and intelligence policy by creating the National Security Council, merging the War and Navy Departments into the Department of Defense, and establishing the Central Intelligence Agency.
- The *Defense Production Act of 1950* (Pub. L. 81-774) is "one of the Nation's primary authorities for ensuring the availability of resources needed for military requirements and civil emergency preparedness and response." (Source: FEMA)
- The *Disaster Relief Act of 1950* (Pub. L. 81-875) was passed "to allow the federal government to provide limited relief to the states during times of man-made or natural disaster ... (including) assistance to alleviate hardships and damages as well as to repair essential public facilities after a major disaster, and to encourage states to develop a disaster plan ... (The) Act gave the local and state governments the first line of official responsibility after a disaster occurs, made the federal response automatic and, for the first time, provided federal agencies the authority to coordinate inter-governmental relief efforts." (Source: Brookings Institution)
- The *Federal Civil Defense Act of 1950* (Pub. L. 81-920) "created the Federal Civil Defense Agency which established the framework for the federal civil defense policy that was used during the 1950's and also provided monetary assistance to states for preparedness activities. The principal focus of this act was protection from nuclear attack but also included plans that dealt with the emergency management and response strategy in case of a natural or man-made disaster." (Source: Brookings Institution)
- The *National Flood Insurance Act of 1968* (Title XIII of the Housing and Urban Development Act of 1968, as amended, Public Law 90-448), as amended, created the National Flood Insurance Program "in response to the rising cost of taxpayer funded disaster relief for flood victims and the increasing amount of damage caused by floods." The NFIP "makes federally backed flood insurance available to homeowners, renters, and business owners" in communities that participate in the program "by adopting and enforcing floodplain management ordinances to reduce future flood damage." (Source: FEMA)
- The *Fire Research and Safety Act of 1968* (Pub. L. 90-259) "established the National Commission on Fire Prevention and Control to investigate the problems with fire the United States was facing and make recommendations ... this commission issued a report titled *America Burning* which recommended drastic measures to lessen the danger fire posed to the United States and called for the establishment of a United States Fire Administration and a national fire training academy." (Source: Brookings Institution)
- The *Robert T. Stafford Disaster Relief and Emergency Assistance Act* ("Stafford Act," Pub. L. 93-288, as amended) "was enacted to support State and local governments and their citizens when disasters overwhelm them. This law establishes a process for requesting and obtaining a Presidential disaster declaration, defines the type and scope of assistance available under the Stafford Act, and sets the conditions for obtaining that assistance." In addition, §404 of the Act establishes the Hazard Mitigation Grant Program (HMGP), which "provides grants to States and local governments to implement long-term hazard mitigation measures after a major disaster declaration ... to reduce the loss of life and property due to natural disasters and to enable mitigation measures to be implemented during the immediate recovery from a disaster." (Source: DHS)
- The *Federal Fire Prevention and Control Act of 1974* (Pub. L. 93-498) "incorporated the *America Burning* recommendations in establishing the National Fire Prevention and Control Administration within the U.S. Department of Commerce;" the NFPCA later became FEMA's United States Fire Administration. (Source: Brookings Institution)
- The *Earthquake Hazards Reduction Act of 1977* (Pub. L. 95-124, as amended) establishes FEMA's National Earthquake Hazard Reduction Program (NEHRP) "to promote the implementation of earthquake hazard reduction measures by the Federal government, as well as State and local governments, National standards and model building code organizations, and the architectural and engineering communities ... Pursuant to the Act FEMA provides grants and technical assistance to facilitate the development of earthquake

preparedness and response plans, and the other Federal NEHRP agencies conduct and fund research into earthquake-related issues." (Source: FEMA)

- The *Department of Defense Authorization Act of 1986* (Pub. L. 99-145, Title 14, Part B) established the Chemical Stockpile Emergency Preparedness Program (CSEPP), in which "FEMA works with the Defense Department in the course of the department's efforts to destroy the United States' stockpile of chemical weapons. FEMA's role in the implementation of this program is to provide assistance to ensure that State and local governments located in the vicinity of the chemical weapons that are being destroyed have adequate emergency preparedness and response plans in place." (Source: FEMA)
- The *Emergency Planning and Community Right-to-Know Act* ("EPCRA", Title III of the *Superfund Amendment and Reauthorization Act of 1986*, Pub. L. 99-499) establishes local and State emergency planning and reporting requirements pertaining to hazardous and toxic chemicals. (Source: EPA)
- Title XXXIV, Subtitle B of the *National Defense Authorization Act for Fiscal Year 1995* (Pub. L. 103-337) incorporated elements of the *Civil Defense Act of 1950* into the Stafford Act to enable FEMA to implement the all-hazards approach to emergency management.
- The *Antiterrorism and Effective Death Penalty Act of 1996* (Pub.L. 104-132) "authorizes the Attorney General, in consultation with the Director of the Federal Emergency Management Agency (FEMA), to provide specialized training and equipment for enhancing the capabilities of metropolitan fire and emergency service departments to respond to terrorist attacks. In response, Justice established the Metropolitan Firefighters and Emergency Medical Services Program." (Source: General Accounting Office)
- The *Defense Against Weapons of Mass Destruction Act of 1996*, better known as the *Nunn-Lugar-Domenici Act* (Pub. L. 104-201, Title XIV) "designates the Department of Defense as the lead agency to enhance domestic preparedness for responding to and managing the consequences of terrorists' use of WMD. Under the act, Defense established the Domestic Preparedness Program to provide first responder training focused on terrorist incidents involving chemical, biological, radiological, and nuclear weapons." (Source: GAO)
- The *Disaster Mitigation Act of 2000* ("DMA 2000," Pub. L. 106-390) amended the *Stafford Act* by repealing the previous mitigation planning provisions (§409) and replacing them with a new set of requirements (§322) that emphasizes the need for State, Tribal, and local entities to closely coordinate mitigation planning and implementation efforts and links the planning requirements to eligibility for several categories of disaster recovery funding. This represents a shift in public policy from an emphasis on post-disaster response to a focus on pre-disaster mitigation, including mitigation planning to prepare for and avoid disasters.
- The *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (the "USA PATRIOT Act," Pub. L. 107-56) was enacted to support the prevention, detection, and prosecution of terrorism through improved coordination of information-sharing, intelligence, and law enforcement.
- The *Aviation and Transportation Security Act of 2001* (Pub. L. 107-71) established the Transportation Security Administration and the Transportation Security Oversight Board.
- The *Homeland Security Act of 2002* (Pub. L. 107-296) established the United States Department of Homeland Security.
- The *Critical Infrastructure Information Act* (the "CII Act," Title II, Subtitle B of the *Homeland Security Act of 2002*) "regulates the use and disclosure of information submitted to ... DHS about vulnerabilities and threats to critical infrastructure." (Source: Congressional Research Service);
- The *Support Anti-terrorism by Fostering Effective Technologies Act of 2002* (the "SAFETY Act," Title VIII, Subtitle G of the *Homeland Security Act of 2002*) was enacted "to ensure that the threat of liability does not deter potential sellers from developing and commercializing technologies that could significantly reduce the risk of, or mitigate the effect of, acts of terrorism." (Source: DHS)

In addition to Congressional action, numerous Executive directives and orders have been promulgated that have shaped the many aspects of what is now collectively referred to as homeland security. These include the following:

- Executive Order 11988, *Floodplain Management* (May 24, 1977), "requires federal agencies to avoid to the extent possible the long and short-term adverse impacts associated with the occupancy and modification of flood plains and to avoid direct and indirect support of floodplain development wherever there is a practicable alternative." The EO states that "each agency shall provide leadership and shall take action to reduce the risk of flood loss, to minimize the impact of floods on human safety, health and welfare, and to restore and preserve the natural and beneficial values served by floodplains in carrying out its responsibilities for (1) acquiring, managing, and disposing of Federal lands, and facilities; (2) providing Federally undertaken, financed, or assisted construction and improvements; and (3) conducting Federal activities and programs affecting land use, including but not limited to water and related land resources planning, regulating, and licensing activities." (Source: FEMA)
- Executive Order 12072, *Federal Space Management* (August 16, 1978), established and maintained the federal policy of locating federal facilities in center cities and urban districts.
- Executive Order 12127, *Federal Emergency Management Agency* (April 1, 1979), implemented Reorganization Plan No. 3 of 1978 (43 FR 41943), creating the Federal Emergency Management Agency. (Source: FEMA)
- Executive Order 12148, *Federal Emergency Management* (July 20, 1979), "merged many of the separate disaster-related responsibilities into a new Federal Emergency Management Agency (FEMA). Among other agencies, FEMA absorbed: the Federal Insurance Administration, the National Fire Prevention and Control Administration, the National Weather Service Community Preparedness Program, the Federal Preparedness Agency of the General Services Administration and the Federal Disaster Assistance Administration activities from HUD. Civil defense responsibilities were also transferred to the new agency from the Defense Department's Defense Civil Preparedness Agency." (Source: FEMA)
- National Security Decision Directive 30, *Managing Terrorist Incidents* (April 10, 1982), identifies Federal agencies' incident management responsibilities and establishes working groups to address various aspects of managing the threat of terrorism.
- Executive Order 12372, *Intergovernmental Review of Federal Programs* (July 14, 1982), requires that "... federal agencies shall provide opportunities for consultation by elected officials of ... state and local governments" in matters relating to security planning. EO 12372 further requires that federal agencies shall "communicate with state and local elected officials as early in the program planning cycle as is reasonably feasible to explain specific plans and actions."
- National Security Decision Directive 207, *National Program for Combating Terrorism* (January 20, 1986), formalized the basic tenets of US terrorism policy, including not making concessions to terrorists, pressuring state sponsors of terrorism, and applying the rule of law such that terrorists are treated as criminals. (Source: GAO)
- Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities* (November 18, 1988), assigns FEMA the responsibilities of "coordinating National Security Emergency Preparedness programs and plans among Federal departments and agencies; coordinating the development of plans, in cooperation with the Secretary of Defense, for mutual civil-military support during National Security Emergencies; and in guiding and assisting State and local governments in achieving preparedness for National Security Emergencies. FEMA also establishes policy and guidance for, and provides assistance to, State and local governments in the coordination of emergency preparedness and response, recovery, and mitigation activities as well as the development and operation of telecommunications and warning systems." (Source: FEMA)
- Executive Order 12657, *Federal Emergency Management Agency Assistance In Emergency Preparedness Planning At Commercial Nuclear Power Plants* (November 18, 1988) provides for FEMA support to "State and local jurisdictions, in cooperation with the operators of licensed commercial nuclear power plants, to ensure they have adequate radiological emergency preparedness plans in place to satisfy the NRC's licensing requirements and to ensure the safety of the public in the vicinity of the plants in the event of an accident at any licensed plant." (Source: FEMA)
- Executive Order 12919, *National Defense Industrial Resources Preparedness* (June 3, 1994), "delegates to the Director of FEMA authorities to use the Defense Production Act (DPA) for emergency preparedness, response, mitigation, and recovery activities. These

authorities include the use of priority orders to divert domestic production and inventories to approved uses." (Source: FEMA)

- Presidential Decision Directive 39, *United States Policy on Counterterrorism* (June 21, 1995), built on NSDD 207 and "elaborated a strategy and an interagency coordination mechanism and management structure to be undertaken by the Federal government to combat both domestic and international terrorism." The Directive designates FEMA as the lead Federal agency for managing the consequences of a terrorist attack and designates the Federal Bureau of Investigation (FBI) as the lead Federal agency for managing the law enforcement response to an attack. (Source: FEMA)
- Executive Order 12977, *Interagency Security Committee* (October 19, 1995), was issued "to improve government-wide coordination of security initiatives. The order created an Interagency Security Committee (ISC), chaired by the Administrator of General Services, and tasked the committee to develop and evaluate security standards for Federal facilities. The ISC is responsible for establishing policies for the security and protection of Federal facilities and is overseeing the implementation of security measures in Federal facilities. The ISC established a number of working groups to address specific security issues. Accomplishments of these groups include a study of minimum security standards for all non-GSA controlled facilities, recommendations for sharing security intelligence, a memorandum of agreement for court security, and draft security design criteria for new construction and modernization projects. (Source: Whole Building Design Guide)
- Executive Order 13010, *Critical Infrastructure Protection* (July 15, 1996), established The President's Commission on Critical Infrastructure Protection (PCCIP) "to formulate a comprehensive national strategy for protecting critical infrastructures." (Source: FEMA)
- Presidential Decision Directive 62, *Combating Terrorism* (May 22, 1998), "reaffirmed PDD 39 and further articulated responsibilities for specific agencies. PDD 62 also established a National Coordinator for Security, Infrastructure Protection, and Counterterrorism, within the National Security Council, to coordinate agencies' programs." (Source: GAO)
- Presidential Decision Directive 63, *Critical Infrastructure Protection* (May 22, 1998), "created a national structure to accomplish the goals laid out in the PCCIP's report. PDD-63 created the office of national coordinator at the National Security Council to ... guide policy for federal agencies and advise nongovernmental entities on protective measures for the nation's information infrastructure. The Critical Infrastructure Assurance Office (CIAO) was formed ... to provide support to the national coordinator's work with government agencies and the private sector in developing a national plan ... To facilitate real-time warnings, PDD-63 established the National Infrastructure Protection Center (NIPC), an interagency unit at the FBI, to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against critical infrastructures." The Directive also created Information Sharing and Analysis Centers and established the National Infrastructure Assurance Council. (Source: National Academies Press)
- Executive Order 13130, *National Infrastructure Assurance Council* (July 14, 1999), established its namesake entity to enhance public-private partnerships in critical infrastructure protection and to encourage private industry to perform periodic risk assessments of critical processes.
- Executive Order 13228, *Establishing the Office of Homeland Security and the Homeland Security Council* (October 8, 2001) created these two organizations within the Executive Office of the President, the former "to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks" and the latter to "serve as the mechanism for ensuring coordination of homeland security-related activities of executive departments and agencies and effective development and implementation of homeland security policies." (Source: EO 13228)
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age* (October 16, 2001), "stated the Bush Administration's policy regarding critical infrastructure protection. EO 13231 also established the President's Critical Infrastructure Protection Board ... to recommend policies and coordinate programs for protecting information systems for critical infrastructures." In addition, the order rescinded Executive Order 13130, replacing the latter's National Infrastructure Assurance Council with the National Infrastructure Advisory Council tasked "to provide advice to the President on the security of information systems for critical infrastructure." (Source: Congressional Research Service)

- Executive Order 13234, *Presidential Task Force on Citizen Preparedness in the War on Terrorism* (November 9, 2001), established the entity of the same name to "identify, review, and recommend appropriate means by which the American public can ... prepare in their homes, neighborhoods, schools, places of worship, workplaces, and public places for the potential consequences of any possible terrorist attacks within the United States (and) volunteer to assist or otherwise support State and local public health and safety officials and others engaged in the effort to prevent, prepare for, and respond to any possible terrorist attacks within the United States."
- The *National Strategy for Homeland Security* (July 16, 2002) establishes an approach for mobilizing and organizing the Nation to secure the U.S. homeland from terrorist attacks. "It provides direction to the federal government departments and agencies that have a role in homeland security. It suggests steps that state and local governments, private companies and organizations, and individual Americans can take to improve our security, and offers incentives for them to do so." (Source: The White House)
- The *National Strategy to Secure Cyberspace* (February 2003) was developed "to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact." (Source: The White House)
- The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (February 2003) was developed to guide the achievement of three strategic objectives: "identifying and assuring the protection of those infrastructure and assets we deem most critical; providing timely warning and assuring the protection of those infrastructures and assets that face a specific, imminent threat; and assuring the protection of other infrastructures and assets that may become targets over time by pursuing specific initiatives and enabling a collaborative environment between the public and private sector." (Source: The White House)

Application of legislation is generally accomplished through the enactment of implementing regulations ("rules"). At the Federal level, these are embodied in the Code of Federal Regulations. Applicable sections include:

- Title 6 (Homeland Security)
 - Part 25: SAFETY Act Regulations
 - Part 29: Protected Critical Infrastructure Information Regulations
- Title 31 (Money and Finance — Treasury)
 - Part 50: Terrorism Risk Insurance Program
- Title 33 (Navigation and Navigable Waters)
 - Part 105: Maritime Security — Facilities
- Title 44 (Emergency Management And Assistance)
 - Part 9: Floodplain Management and Protection of Wetlands
 - Part 10: Environmental Considerations
 - Part 25: Uniform Relocation Assistance and Real Property Acquisition for Federal and Federally Assisted Programs
 - Part 60: Criteria for Land Management and Use
 - Part 65: Identification and Mapping of Special Hazard Areas
 - Part 71: Implementation of Coastal Barrier Legislation
 - Part 78: Flood Mitigation Assistance
 - Part 201: Mitigation Planning
 - Part 300: Disaster Preparedness Assistance
 - Part 302: Civil Defense-State and Local Emergency Management Assistance Program (EMA)
 - Part 312: Use of Civil Defense Personnel, Materials, and Facilities for Natural Disaster Purposes
 - Part 323: Guidance on Priority Use of Resources in Immediate Post Attack Period

- Part 350: Review and Approval of State and Local Radiological Emergency Plans and Preparedness
- Part 351: Radiological Emergency Planning and Preparedness
- Part 352: Commercial Nuclear Power Plants: Emergency Preparedness Planning
- Part 361: National Earthquake Hazards Reduction Assistance to State and Local Governments
- Title 49 (Transportation)
 - Part 1520: Protection of Sensitive Security Information
 - Part 1542: Airport Security

While not carrying the force of law as regulations do, standards constitute established, widely accepted practices. Standards applicable to homeland security include:

- National Fire Protection Association
 - [NFPA 730](#), *Guide for Premises Security* (proposed)
 - [NFPA 731](#), *Standard for the Installation of Electronic Premises Security Systems* (proposed)
 - NFPA 1600, *National Preparedness Standard on Disaster/Emergency Management and Business Continuity Programs*
- ASTM International (Committee E54, Homeland Security Applications)
 - WK 5498, *Standard Guide for Developing Model Emergency Operations Plans in Response to All-Hazard Events Including CBRNE*
 - WK 5515, *Standard Guide for Establishing a Health Risk-Based Event-Specific Process for deriving Restoration Levels for High-Value Property*
 - WK 5516, *Standard Guide for Building Event Dispersion and Health Assessment Preparedness and Response Planning*
 - WK 5248, *Standard Guide for Selection of Exterior Intrusion Detection Sensors*
 - WK 5249, *Standard Guide for Selection of Interior Intrusion Detection Sensors*
 - WK 5250, *Standard Guide for the Selection of Physical and Electronic Security Command and Control Systems*
 - WK 4699, *Standard Practice for the Control and Evaluation of a Contaminated Site*
 - WK 5394, *Standard Test Method for Materials used to Stabilize Radioactive Particulate Spread after a Radiological Event*
 - WK 6350, *Standard Test Method for Determining the Decontamination Efficacy of Treatments for Removing Radionuclides from Building Surfaces*
 - WK 6352, *Test Method for Determination of Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability*
 - WK 6376, *Standard Test Method for Determining the Activity of Incorporated Antimicrobial Agent(s) In Polymeric or Hydrophobic Materials*
 - WK 4867, *Guide to Relating Protection Levels A, B, C and D to National Fire Protection Association Protection Levels*
 - WK 5320, *Standard Specification for Chemical Protection using Permeable, Semi-Permeable or Impermeable Materials*
 - WK 3799, *Standard Guide for the Selection of Antiterrorism Physical Security Measures for Buildings*
- ASCE / ANSI
 - ANSI/ASCE 7-98, *Minimum Design Loads for Buildings and Other Structures* (January 2000)

At the operational level, several sources exist for security planning guidance. Among these, the military and diplomatic communities have been concerned for the longest time with site- and facility-level security. However, following the 1995 bombing of the Murrah Federal Building in

Oklahoma City, Oklahoma, security began receiving significantly greater attention from federal civilian facilities managers as well. Finally, following the terrorist attacks of September 11, 2001, security crossed over into the state, tribal, local, and private-sector arenas. Today, a design guidance library should include:

- The Department of Defense Unified Facilities Criteria (UFC) family of documents "provide planning, design, construction, sustainment, restoration, and modernization criteria, and apply to the Military Departments, the Defense Agencies, and the DoD Field Activities ... Headquarters, United States Army Corps of Engineers (HQUSACE), Naval Facilities Engineering Command (NAVFAC), and Air Force Civil Engineer Support Agency (AFCESA) are responsible for administration of the UFC system." The UFC include guidance documents addressing master planning, site planning and design, standoff, and antiterrorism/force protection design issues. (Source: US Army Corps of Engineers) However, as the DOD standards establish minimum standoff distances (i.e. building setbacks) as the "primary strategy" for the protection of buildings and facilities used by the military, their applicability may be somewhat limited in urban settings or in other areas where economic and/or design constraints do not allow for the reservation of significant amounts of open space.
- Perhaps the first major guidance for the civilian community was developed by the U.S. Department of Justice in the wake of the 1995 bombing of the Murrah Federal Building in Oklahoma City, Oklahoma. *Vulnerability Assessment of Federal Facilities* "produced recommended minimum standards for security at federal facilities ... divided Federal sites into five security levels ranging from Level 1 (minimum security needs) to Level 5 (maximum) ... [and] listed recommendations for upgrading federal building security, including 52 security standards addressing such items as parking, lighting, physical barriers, and closed circuit television monitoring." (Source: GSA, Office of the Chief Architect)
- Soon after the DoJ report, the General Services Administration (GSA) began promulgating the *Facilities Standards for the Public Buildings Service*, which "establishes design standards and criteria for new buildings, major and minor alterations, and work in historic structures for the Public Buildings Service ... This document contains policy and technical criteria to be used in the programming, design, and documentation of GSA buildings." Section 8 of the *Facilities Standards* addresses security design issues. (Source: GSA, OCA)
- The U.S. Government's Interagency Security Committee (ISC) "was established by Executive Order 12977 of October 19, 1995 to develop long-term construction standards for locations requiring blast resistance or other specialized security measures. In a series of working group discussions, the ISC revised and updated GSA's 1997 Draft Security Criteria, taking into consideration technology developments, new cost considerations, the experience of practitioners applying the criteria, and the need to balance security requirements with public building environments that remain lively, open, and accessible ... [the ISC] developed the ISC Security Design Criteria to ensure that security becomes an integral part of the planning, design, and construction of new Federal office buildings and major modernization projects. The criteria consider security in all building systems and elements." (Source: GSA, OCA)
- Finally, the Federal Emergency Management Agency (FEMA) has developed a family of guidance products that are based on the latest military and government standards but are designed to meet the broader needs of the State, Tribal, local, and private sectors. FEMA Publication 386-7, *Integrating Manmade Hazards into Mitigation Planning*, addresses special considerations that can arise when security and antiterrorism are addressed at the community planning level, including discussions about public participation, information security, interdisciplinary planning, prioritization of mitigation actions, and project funding. FEMA's Risk Management Series of publications (RMS) is more technical in nature, comprising FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*; FEMA 427, *Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks*; FEMA 428, *Primer to Design Safe School Projects in Case of Terrorist Attacks*; and FEMA 429, *Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings*. Additional volumes will be released in 2005, including FEMA 430, *Primer for Incorporating Building Security Components in Architectural Design*; FEMA 452, *Methodology for Preparing Threat Assessments for Commercial Buildings*; FEMA 453, *Multihazard Shelter (Safe Havens) Design*; FEMA 455, *Rapid Visual Screening for Building*

Security; and FEMA 459, *Incremental Rehabilitation to Improve Security in Buildings*.
(Source: FEMA)

No discussion of security planning would be complete without some treatment of the issue of information sensitivity. The first challenge related to information sensitivity is the need to determine exactly what information should be considered sensitive. In many cases, information can be categorically determined to be sensitive; for example, there is no circumstance under which it would be appropriate to publicly release information on the security vulnerabilities of critical infrastructure installations. Examples of federal categorical designations include:

- 6 CFR Part 29, which designates information on vulnerability of critical infrastructures "Protected Critical Infrastructure Information (PCII)" and protects it from disclosure using Freedom of Information Act exemption 3 (source: Department of Homeland Security)
- 18 CFR Part 388, which designates as Critical Energy Infrastructure Information (CEII) "information concerning proposed or existing critical infrastructure (physical or virtual) that: relates to the production, generation, transportation, transmission, or distribution of energy; could be useful to a person in planning an attack on critical infrastructure; is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552; and gives strategic information beyond the location of the critical infrastructure." (Source: Federal Energy Regulatory Commission)
- 49 CFR Part 15, which defines the category of "Sensitive Security Information (SSI)" as comprising information on transportation-related security programs and contingency plans, security directives, threat information circulars, performance specifications, vulnerability assessments, and security inspection or investigative information. (Source: Transportation Security Administration)
- In addition, the Freedom of Information Act (FOIA) contains several statutory disclosure exemptions that, while they do not inherently comprise categories of sensitive information, provide useful insight into the types of information that may be considered sensitive.
- Another resource that can help in determining whether to withhold information is the Federal Geographic Data Consortium's *Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns*. Although the document's scope is constrained to geospatial information, the decision structure it provides is broadly applicable and can assist decision makers in evaluating their options for controlling its promulgation. Similarly, the RAND Corporation's report *Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information* describes the information "supply and demand" factors involved in evaluating adversaries' potential data needs against the universe of data that currently exists in the public domain, helping decision makers to identify the usefulness of information to an adversary, the information's uniqueness in the public domain, and the societal benefits and costs associated with its restriction.

Note that when evaluating information sensitivity, it is also important to recognize that bits of information that seem to be innocuous in and of themselves can be aggregated to reveal a larger, more damaging picture; thus, each bit of information should be evaluated not only on its face but also in light of how it may compound the utility of other bits of information when in the hands of an adversary.

Once it has been determined that the sensitivity of an element of information merits disclosure restrictions, the challenge then becomes determining the most appropriate and effective means for controlling its dissemination. The federal government has the option of classifying information and has an extensive portfolio of laws, regulations, Executive Orders, policies, procedures, and guidance on how classified information is to be managed. Although this tool is not available to state, tribal, local, and private-sector entities, numerous other options are at their disposal. At the statutory level, for example, state, tribal, and local governments may establish exemptions to their disclosure laws (often called "sunshine" laws) to protect information. Jurisdictions that employ such measures include:

- Alaska, where state law exempts from disclosure "records or information pertaining to a plan, program, or procedures for establishing, maintaining, or restoring security in the

state, or to a detailed description or evaluation of systems, facilities, or infrastructure in the state, but only to the extent that the production of the records or information (A) could reasonably be expected to interfere with the implementation or enforcement of the security plan, program, or procedures; (B) would disclose confidential guidelines for investigations or enforcement and the disclosure could reasonably be expected to risk circumvention of the law; or (C) could reasonably be expected to endanger the life or physical safety of an individual or to present a real and substantial risk to the public health and welfare."

- North Carolina, where the state's public records law was amended in January 2002 such that information "containing specific details of public security plans and ... the detailed plans and drawings of public building and infrastructure" is no longer considered public information and can be restricted. Pursuant to the amended state law, the City of Greensboro enacted its own Infrastructure Information Security Policy, with an effective date of July 1, 2004.
- Utah, where state law protects records the disclosure of which would jeopardize the life or safety of an individual or would jeopardize the security of governmental property, governmental programs, or governmental recordkeeping systems from damage, theft, or other appropriation or use contrary to law or public policy.

In addition to legislation, personnel practices and information handling protocols can go a long way toward protecting information from inadvertent or inappropriate disclosure. Ensuring rigorous background investigations for planning personnel, restricting the distribution of sensitive information to those with a "need to know," and the use of non-disclosure agreements are useful measures that can be implemented at any level of government and in the private sector. Furthermore, jurisdictions are encouraged to develop and implement a formal policy on the designation, handling, and storage of sensitive information. A good example of such a policy is the U.S. Department of Homeland Security's Management Directive 11042, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*.

Finally, the need for Operations Security (OPSEC) is not limited to those who work with classified information. OPSEC is " a process used to deny to potential adversaries information about capabilities and/or intentions by identifying, controlling and protecting evidence of the planning and executing of sensitive activities. This process is equally applicable to government, its contractors, and to private enterprise in the protection of their trade secrets and other proprietary information." (Source: OPSEC Professionals Society) Anyone dealing with sensitive information should understand the ease with which it can leak from an individual or an organization. OPSEC guidance is available from the following sources:

- The Interagency OPSEC Support Staff (IOSS), which primarily serves the Federal government community but provides widely applicable information (www.ioass.gov).
- The OPSEC Professionals Society, which publishes an annual journal and offers professional certification in Operations Security (www.opsec.org).